Administrator's Guide

HP ArcSight Management Center 1.0

September 30, 2013

ArcSight
An HP Company

Contact Info

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI.
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Revision
9/30/2013	Initial release.

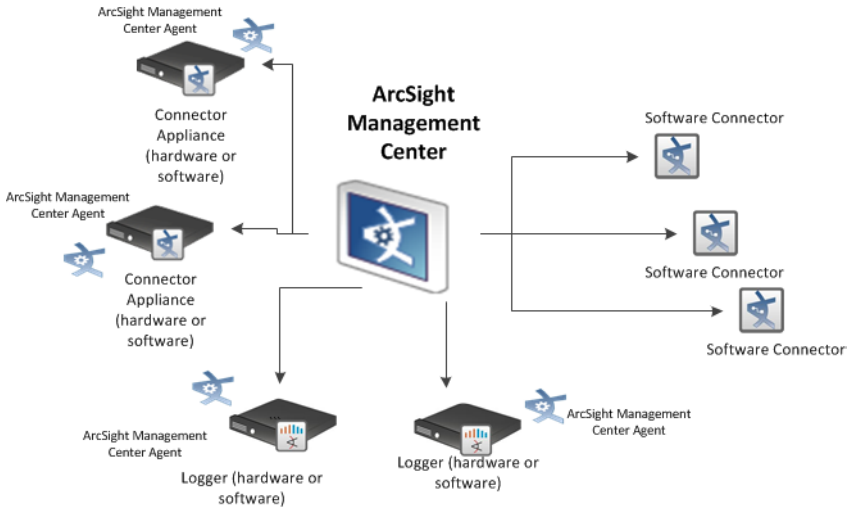
Contents

Chapter 1

HP ArcSight Management Center Overview

The following topics are discussed here.

HP ArcSight Management Center 1.0 provides centralized management for Connector Appliances, Loggers, and software connectors with a single panel view of all managed ArcSight products.



HP ArcSight Management Center Features

HP ArcSight Management Center includes these features:

- **Configuration Creation and Pushing:** Create or import configurations for managed products, and then rapidly push them to products of the same type across your network, ensuring consistent configuration for managed products with one action. Configurations include System Admin settings, Logger settings, Connector Appliance settings, and Connector settings.
- **Remote and Bulk Management of ArcSight Products:** Perform a variety of remote management tasks on ArcSight products, singly and in bulk, including Connector Appliances, Loggers, containers, and software connectors.
- **Add Hosts to Create Multiple Managed Nodes Quickly:** Add a host to ArcSight Management Center to quickly add all the nodes associated with the host in one

action. For example, if you add a Connector Appliance host to ArcSight Management Center, all of its containers and managed software connectors are added at the same time.

- **Monitoring:** Monitor the performance of **ArcSight Management Center** with a variety of criteria and over different time intervals.
- **System Backup and Restore:** Perform automatic backups of your ArcSight Management Center configuration and restore them as needed.
- **Take System Snapshots:** Take a snapshot of your current ArcSight Management Center to produce troubleshooting logs.
- **Manage Repositories:** Create and manage repositories to store logs, CA certificates, and other important files, and retrieve these files quickly.

Chapter 2

Installation

This chapter describes how to install ArcSight Management Center and the ArcSight Management Center Agent.

The following topics are discussed here.

ArcSight Management Center Installation Process

Browser Requirements

ArcSight Management Center uses a web-based user interface. Refer to the ArcSight Management Center Release Notes, available from the HP ArcSight community, Protect724, for current information on supported platforms, supported browsers, and other technical requirements.

Changing the Default Password

After initial setup is complete, change the default password to a secure password. To change the default password, follow the instructions in Chapter 11, Change Password, on page 163.

For added security, rename the default admin username to a secure name. To change a username, follow the instructions under **To edit a user** in Chapter 11, User Management, on page 158.

The ArcSight Management Center Agent

After installing ArcSight Management Center, you may need to install the ArcSight Management Center Agent on any of the following node types you intend to manage:

- *Connector Appliance or Logger Appliance:* The ArcSight Management Center Agent is installed automatically on these node types when they are remotely managed with ArcSight Management Center. No manual installation steps are required.
- *Software Connector Appliance or Software Logger:* Transfer or copy the ArcSight Management Center Agent installer to these node types, and then install the Agent

manually. For more information on manual ArcSight Management Center Agent installation, see “Installing the ArcSight Management Center Agent” on page 26.

Software connectors do not require installation of the ArcSight Management Center Agent.

Installing ArcSight Management Center

The following section provides instructions to install ArcSight Management Center.

Prerequisites for Installation

Please note the following prerequisites before beginning the installation process.

- You can install ArcSight Management Center as a root or non-root user. However, when installing as a root user, a non-root user account is required, in order to run some required processes.
- When installing the ArcSight Management Center as a root user, you can select the port on which it listens for secure web connections (HTTPS). Note that when installed as a non-root user, the port must be configured to 9000. This value cannot be changed and must be externally accessible.
- If installed as a root user, ArcSight Management Center can be configured to start as a service.
- For Apache to start, the ArcSight Management Center hostname must be resolvable. Add your hostname to either `/etc/hosts` or DNS.

Installing a License for ArcSight Management Center

A valid license is required for ArcSight Management Center. A license file is uniquely generated for each download; therefore, you cannot use the same license file to install multiple instances of the product.

To obtain the license, follow the instructions in the *Electronic Delivery Receipt* you received from HP in an email after placing your order.

Installation Modes

You can install ArcSight Management Center in these modes:

- **GUI** – A wizard steps you through the installation and configuration process. For detailed information, see “GUI Mode Installation” on page 15.

If you are using a Windows system to connect to the machine where ArcSight Management Center is to be installed, and prefer to install in GUI mode, you must connect use an X Window client, such as Xming for Windows.

- **Console** – A command-line process steps you through the installation and configuration process. See “Console Mode Installation” on page 18 for detailed instructions.
- **Silent** – An option that enables scripting of the installation process. There is no need to interact with the installer, as you provide the installation and configuration input through a file. See “Silent Mode Installation” on page 20 for detailed instructions.

Installation Steps

This section describes ArcSight Management Center steps for each mode.

GUI Mode Installation

You can install ArcSight Management Center as a root user or as a non-root user. See "Prerequisites for Installation" on page 14 for details and restrictions.

To install ArcSight Management Center using the GUI mode:

1. Make sure the machine on which you install ArcSight Management Center complies with the requirements listed in the ArcSight Management Center Release Notes (available from the HP ArcSight community, Protect724).

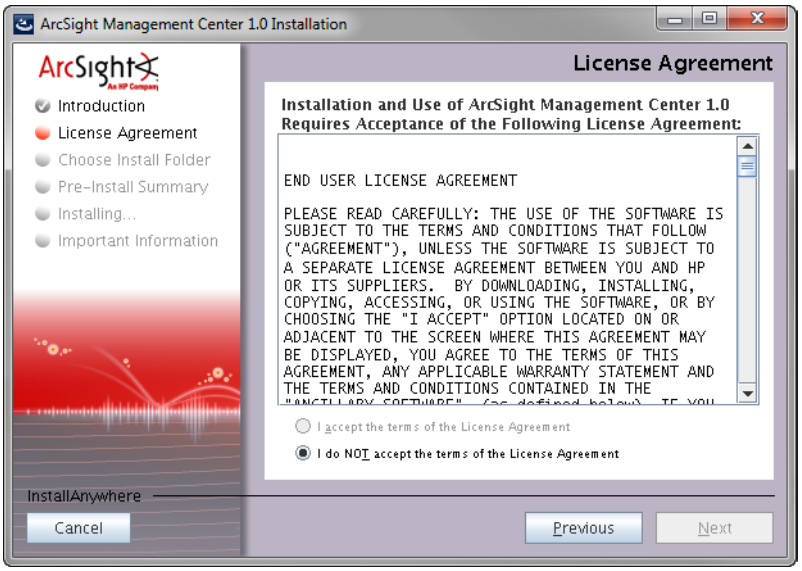
2. Run these commands from the directory where you copied the ArcSight Management Center software:

   ```
   chmod +x ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin
   ```

   ```
   ./ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin
   ```

   The installation wizard starts. Review the dialog box, and then click **Next**.

3. Review the License Agreement details. Click **I accept the terms of the License Agreement**. Then, click **Next**.

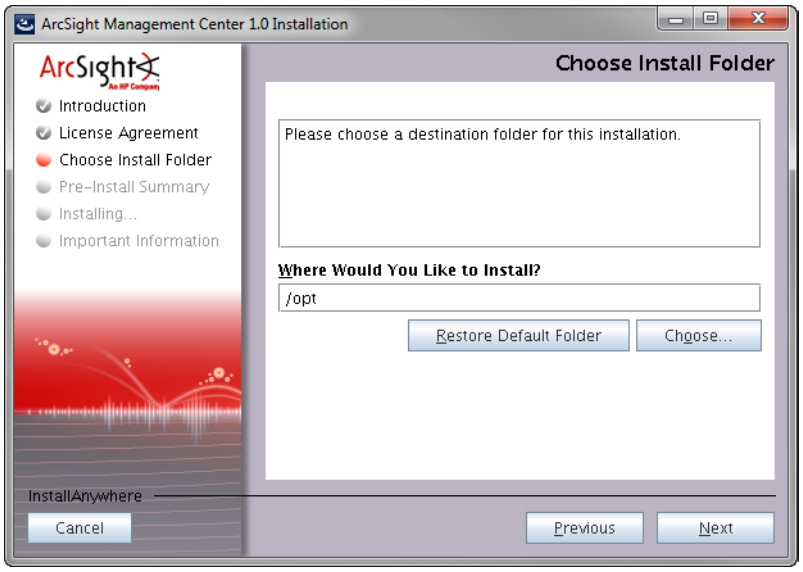


> **Tip**
>
> To accept the License Agreement, scroll down to the end of the License Agreement details.

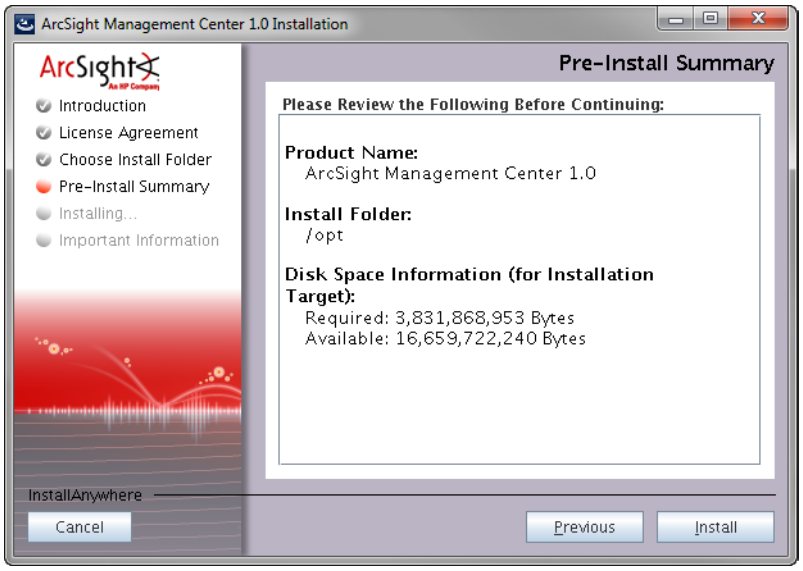
4. Specify or browse to a folder where you want to install ArcSight Management Center, as shown below. By default, `/opt` is specified.

> **Note**
>
> The default installation directory is `/opt`. However, you should specify a new installation directory in `/opt` that will easily identify ArcSight Management Center files, such as `/opt/arcmc`, to distinguish them from files associated with other HP ArcSight products.

If there is insufficient space in the location you specify for installation, an error message appears. You need to either specify a different location or make adequate space in the location you specified before installation can proceed.

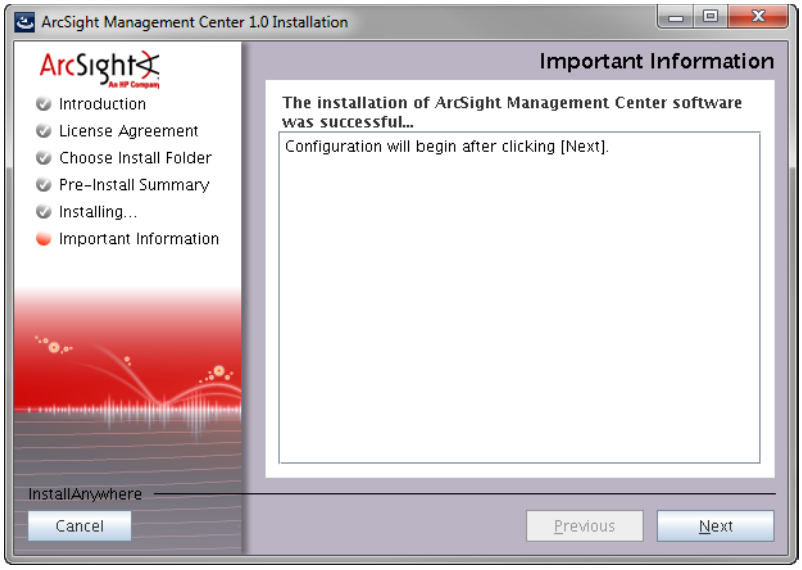


5 Review the summary of installation information on the Pre-Installation Summary dialog, and then click **Install**.



The ArcSight Management Center software begins the installation process.

6 When installation is complete, click **Next** to begin the configuration wizard.



7 If you run the ArcSight Management Center software installer as a root user, the next dialog enables you to specify a non-root user (which must exist on the system already) and to configure a port on which ArcSight Management Center users will connect through the UI.

For example, you can enter 443, the standard HTTPS port, or any other that suits your needs. If any port other than 443 is specified, users will need to enter the port number in the URL they use to access the ArcSight Management Center UI.

Note

Please note that the values you enter in the next step cannot be changed later in the process.

Enter the user name of the non-root user and the HTTPS port number, and then click **Next**.

8 After the software is installed, click **Next** to begin ArcSight Management Center initialization.

9 After initialization is complete, click **Done** to launch the ArcSight Management Center Configuration wizard.

Note

The Configuration wizard should launch automatically. If it does not, use this command to launch the wizard:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup
```

10 If you have run the ArcSight Management Center software installer as a root user, the next dialog enables you to configure ArcSight Management Center to run as a system service. By default, ArcSight Management Center runs as a standalone application, requiring a manual launch.

When you install ArcSight Management Center as a root user, a service called `arcsight_arcmc` can be configured, created, and enabled at runlevel 3 and 5.

Additionally, a few libraries are added using `ldconfig`. For a complete list of those libraries, see `/etc/ld.so.conf.d/arcsight_arcmc.conf` and `<install_dir>/current/arcsight/install/ldconfig.out`.

11 You have installed ArcSight Management Center. Click **Start** ArcSight Management Center **Now**, or click **Start** ArcSight Management Center **later,** and then click **Finish**.

If you have selected to start ArcSight Management Center later, read the information in "Starting and Stopping ArcSight Management Center" on page 24 to understand how to start ArcSight Management Center at a later time.

12 If you selected **Start** ArcSight Management Center **Now**, click **Finish** to exit the wizard. Alternatively, wait for the next dialog which provides the URL to access the ArcSight Management Center interface.

ArcSight Management Center continues to start services and processes in the background. If you have selected to continue within the wizard, follow the instructions on the dialog or use the instructions in "Connecting to the ArcSight Management Center User Interface" on page 23 to connect to the ArcSight Management Center.

Console Mode Installation

You can install ArcSight Management Center as a root user or as a non-root user. See "Prerequisites for Installation" on page 14 for details.

To install ArcSight Management Center using the Console mode:

1 Make sure the machine on which you install ArcSight Management Center complies with the requirements listed in the ArcSight Management Center Release Notes.

2 Run these commands from the directory where you copied the ArcSight Management Center software:

```
chmod +x ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin

./ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin -i
console
```

The installation wizard starts in command-line mode, as shown below. Press **Enter** to continue.

```
Introduction
------------

InstallAnywhere will guide you through the installation of
ArcSight Management Center.

It is strongly recommended that you quit all programs before
continuing with this installation.

Respond to each prompt to proceed to the next step in the
installation. If you want to change something on a previous
step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

3 After the license information displays, press **Enter** until you see the following information:

```
Select "I accept the terms of the License Agreement" below if
you recognize that you have read the terms of this Agreement and
attachments and agree to be bound by each of these terms.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):Y
```

4 Go through the following prompts, from `Choose Install Folder` to `Intervention Required`, pressing **Enter** to continue through until the following confirmation appears:

```
================================================================
================

Important Information

---------------------


The installation of ArcSight Management Center software was
successful.


Configuration will begin after pressing [Enter].


PRESS <ENTER> TO CONTINUE:
```

```
================================================================
================

Intervention Required

---------------------


Values entered below may not be changed later in the process.


Enter a non-root user account (DEFAULT: ): <non-root user>


Enter an HTTPS port (default is 443) (DEFAULT: 443):
```

```
================================================================
================

Important Information

---------------------


The configuration of ArcSight Management Center software was
successful.


Initialization will begin after pressing [Enter]. This may take
several

minutes.


PRESS <ENTER> TO CONTINUE:
```

```
================================================================
================

Important Information

---------------------


The initialization of ArcSight Management Center software was
successful.
```

The prompts that follow are the same as the ones described for the GUI mode install in "GUI Mode Installation" on page 15. Follow the instructions provided for the GUI mode install to complete the installation.

If ArcSight Management Center is installed in Console mode, it will be uninstalled in Console mode as well. See "Uninstalling in Console Mode" on page 25 for more information.

Silent Mode Installation

Silent mode enables scripting of the installation process. Before you install ArcSight Management Center in silent mode, create two properties files required for the silent mode installation:

- A file to capture the installation properties
- A file to capture the configuration properties

After you have generated the two files, you need to merge them into one file and use the resulting file for silent mode installations.

About Licenses for Silent Mode Installations

As for any ArcSight Management Center installation, each silent mode installation requires a unique license file. Obtain licenses from HP Customer Support and place them on the machines on which you will be installing in silent mode, or ensure that the location where the license is placed is accessible from those machines.

Generating the Silent Install Properties File

This procedure generates the two properties files and then instructs you to combine them into one file. The resulting file is used for future silent installations.

1. Log in to the machine on which you wish to generate the installation properties file.

   If you want the silent mode installations to be done as root user, log in as root in this step. Otherwise, log in as a non-root user.

2. Run this command:

   ```
   ./ArcSight-arcmc-
   1.0.0.<installer_build_number><installer_build_number>.0.bin -r
   <directory_location>
   ```

   where `<directory_location>` is the location of the directory where the generated properties file will be placed. This cannot be the same location where ArcSight Management Center is being installed.

   The properties file is called `installer.properties`. You *cannot* change this name.

3. Install ArcSight Management Center in GUI mode, as described in "GUI Mode Installation" on page 15 until you arrive at step 10.

   At Step 10 of the installation procedure, do the following:

   a. Click **Previous** instead of clicking **Done** to proceed further.

   b. Then, click **Cancel** to stop the installation.

4. When the confirmation message appears, click **Cancel**. Click **Quit** to clear this message.

5. Navigate to the directory location you specified for the `installer.properties` file earlier.

   The following is an example of the generated `installer.properties` file.

   ```
   # Replay feature output

   # ---------------------

   # This file was built by the Replay feature of InstallAnywhere.

   # It contains variables that were set by Panels, Consoles or
   Custom Code.




   #Choose Install Folder

   #---------------------
   ```

```
USER_INSTALL_DIR=/opt/<arcmc_installation_folder>/<build
number>/installdir


#Install

#-------

-fileOverwrite_/opt/<arcmc_installation_folder>/<build
number>/installdir/UninstallerData/Uninstall_ArcSight_Managemen
t_Center_1.0.lax=Yes


#Intervention Required

#---------------------

USER_AND_PORT_1=username

USER_AND_PORT_2=443
```

6 Start the configuration wizard with the option to record configuration properties:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup -i
recorderui
```

When prompted to enter a file name to capture the configuration properties, enter a meaningful name; for example, `config.properties`, and then browse to choose the same directory as the `installer.properties` file.

7 Step through the configuration wizard, as described starting at **Step 10** of "GUI Mode Installation" on page 15.

8 After the configuration properties file is generated, append the contents of this file to the `installer.properties` file generated in the previous procedure, Generating the Silent Install Properties File, to create a combined file.

For example, you can use the cat command to concatenate both files:

```
cat installer.properties config.properties >
<combinedproperties.properties>
```

9 Include the following property in the combined file:

```
ARCSIGHT_CONAPP_SETUP_PROPERTIES=<directory_location>/
<combined_properties_file>
```

where `<directory_location>` is the path of the directory where the combined file is located, and `<combined_properties_file>` is the file name of the combined file you created earlier.

Use the combined file for future ArcSight Management Center silent mode installations, as described in Installing Using the Generated Properties File below.

Installing Using the Generated Properties File

To install ArcSight Management Center using Silent mode, do the following.

1 Uninstall the previously installed version of ArcSight Management Center, as explained in "Uninstalling ArcSight Management Center" on page 25

2 Make sure the machine on which you install ArcSight Management Center complies with the requirements listed in the HP ArcSight Management Center Release Notes, and the prerequisites listed in "Prerequisites for Installation" on page 14.

3 Copy the combined properties file you generated previously to the location where you have copied the ArcSight Management Center software.

4 Edit the `licensePanel.path` property in the silent mode properties file to include the location of the license file for this instance of the installation. (A unique license file is required for each instance of installation.)

OR

Set the `licensePanel.path` property to point to a file, such as `arcmc_license.zip`. Then, for each instance of the silent mode installation, copy the relevant license file to the location and rename it to `arcmc_license.zip`. Doing so will avoid the need to update the combined properties file for each installation.

5 Run these commands from the directory where you copied the ArcSight Management Center software:

```
chmod +x ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin
```

```
./ArcSight-arcmc-1.0.0.<installer_build_number>.0.bin -i silent
-f <combined_properties_file>
```

The rest of the installation and configuration proceeds silently without requiring further input.

ArcSight Management Center Processes

After installation, the following processes run as part of ArcSight Management Center:

- `apache`
- `aps`
- `postgresql`
- `web`

Connecting to the ArcSight Management Center User Interface

Because the ArcSight Management Center user interface uses SSL, make sure you connect to it using this URL:

```
https://<hostname or IP address>:<configured_port>
```

where `hostname` or `IP address` is the system on which you installed ArcSight Management Center. If ArcSight Management Center was installed as root and the default port was used, then `<configured_port>` is optional.

If you are connecting for the first time, use the following default credentials:

```
Username: admin
```

```
Password: password
```

Change the credentials as soon as possible after connecting to your ArcSight Management Center for the first time or before deploying the system in production.

Starting and Stopping ArcSight Management Center

The `arcmcd` command enables you to start or stop the ArcSight Management Center software process. In addition, the command includes a number of parameters that you can use to control other processes that run as part of the ArcSight Management Center software.

If your ArcSight Management Center is installed to run as a system service, use this command to start, stop, or check the status of a process on ArcSight Management Center.

```
<install_dir>/current/arcsight/arcmc/bin/arcmcd
{start|stop|restart|status|quit}

<install_dir>/current/arcsight/arcmc/bin/arcmcd {start
<process_name> | stop <process_name> | restart <process_name>}
service arcsight_arcmc {start | stop | status}
```

The following table describes commands for `arcmcd`.

Table 2-1 `arcmcd` **Commands**

Command	Purpose
`arcmcd start`	Start all processes listed under the System and Process sections in the figure above. **Use this command to launch** ArcSight Management Center.
`arcmcd stop`	Stop processes listed under the Process section only. Use this command when you want to leave the ArcSight Management Center process running but stop all other processes.

`arcmcd restart`	This command restarts processes listed under the Process section only.
	Note: When the `arcmcd restart` command is used to restart the ArcSight Management Center service and process, the status message for the `aps` process displays this message:
	`Process 'aps' Execution failed.`
	The status and message change to the expected message after a few seconds:
	`Process 'aps' running.`

`arcmcd status`	Display the current status of all processes.
`arcmcd quit`	Stops all processes listed under the System and Process sections in the figure above. Use this command to stop ArcSight Management Center.
`arcmcd start <process_name>`	Start the named process. For example, `arcmcd start apache`
`arcmcd stop <process_name>`	Stop the named process. For example, `arcmcd stop apache`

Table 2-1 `arcmcd` **Commands**

Command	Purpose
`arcmcd restart <process_name>`	Restart the named process. For example, `arcmcd restart apache`

Uninstalling ArcSight Management Center

Uninstall ArcSight Management Center in the same user mode in which the installation was performed. For example, if you performed the installation as root, then you must perform the uninstallation as root

Uninstalling in GUI Mode

To uninstall ArcSight Management Center in GUI mode, enter this command in the directory where you installed ArcSight Management Center:

```
<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_1.0
```

The uninstall wizard starts. Click **Uninstall** to start uninstalling ArcSight Management Center and follow the prompts in the wizard.

If using GUI mode and uninstalling ArcSight Management Center software over an SSH connection, make sure that you have enabled X window forwarding using the **-X** option, so that you can view the screens of the uninstall wizard.

If using PuTTY, you also need an X11 client on the machine from which you are connecting to the Linux machine.

Uninstalling in Console Mode

If you installed ArcSight Management Center in Console mode, then, by default, uninstallation occurs in Console mode.

To uninstall in Console mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_1.0`
2. At the prompt, press **Enter** again to confirm uninstallation. The application will be uninstalled.

Uninstalling in Silent Mode

If you installed ArcSight Management Center in Silent mode, then, by default, uninstallation occurs in Silent mode.

To uninstall in Silent mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_1.0`. The application will be uninstalled without further interaction.
2. After uninstalling, manually delete the `/userdata` directory.

Enabling or Disabling ArcSight Management Center as a System Service

If you want to disable ArcSight Management Center from starting as a system service, or if you want to enable it to start as a system service after it has been installed, follow these steps.

This option is only accessible to root users.

1. Ensure you are logged in as a root user on the system on which ArcSight Management Center is installed.
2. Do one of the following:

   For GUI mode, run:
   `<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup`

   or

   For Console mode, run:
   `<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup –i console`
3. Select **Change ArcMC system service settings**, and then click **Next**.
4. If ArcSight Management Center is currently installed as a service, the next dialog provides you the option to disable it. If ArcSight Management Center is currently installed as a standalone application, you can configure it to run as a service.
5. Click **Finish**.

Installing the ArcSight Management Center Agent

The ArcSight Management Center Agent runs on managed hosts and enables their management by ArcSight Management Center. Whether you need to install the ArcSight Management Center on a host depends on the host's form factor.

For Appliance Hosts

When adding an appliance (Connector Appliance or Logger Appliance) as a host, ArcSight Management Center automatically pushes the ArcSight Management Center Agent installer to the appliance, installs it, and then starts the service.The appliance is then ready to manage in ArcSight Management Center. You won't need to take any manual installation steps.

For Software Connector Appliances or Software Loggers

Before adding Software Connector Appliance or Software Logger hosts to ArcSight Management Center, you must first manually transfer the ArcSight Management Center Agent installer to the application host. Then, run the installer. Completion of the installation

will automatically start the Agent. You can then add the host to ArcSight Management Center.

For information on adding hosts to ArcSight Management Center, see Chapter 5, About Adding Hosts, on page 49.

For Software Connectors

Software connectors do not require the ArcSight Management Center Agent.

Manual Installation Procedure

You need to transfer, copy, or download the ArcSight Management Center Agent installer file to any Software Logger or Software Connector Appliance you intend to add for management. (You can use any file transfer utility, such as FTP.) You must then manually run the Agent installer on the host and complete the installation.

The ArcSight Management Center Agent and the managed application must both be installed using the same user mode. For example, if the Software Logger to be managed is installed as a root user, then the ArcSight Management Center Agent must also be installed as a root user.

To manually install the ArcSight Management Center Agent on Software Connector Appliance or Software Logger:

1 In the directory to where you transferred the installer, run these commands:

```
chmod +x ArcSight-ArcMcAgent-
1.0.0.<installer_build_number>.0.bin

./ArcSight-ArcMcAgent-1.0.0.<installer_build_number>.0.bin
LAX_VM <installation_directory>/current/local/jre/bin/java
```

where `<installation_directory>` is the installation directory of the Software Appliance or Software Logger.

The installation wizard starts. Review the dialog box, and then click **Next.**The required installation path is the install directory (that is, the same directory where Software Connector Appliance or Software Logger is installed).

2 Follow the prompts to complete the installation. The Agent is automatically started upon completion of the installation process.

Starting, Stopping, or Restarting the Agent

After installation, the `arcmcagent` process runs on the host. This process automatically starts after either automatic or manual installation. However, if the Agent stops for any reason, it can be manually started.

To manually start, stop, or restart the Agent:

1 On the Connector Appliance or Logger GUI, click **Setup > System Admin > Process status**.

2 Select *arcmcagent* from the list of processes.

3 Click **Start | Stop | Restart.**

On Software Connector Appliance or Software Logger (only)

To manually start or stop the Agent on Software Connector Appliance or Software Logger:

1 Run
`<install_dir>/current/arcsight/<conapp|logger>/bin/<conappd|loggerd> <start|stop> arcmcagent`

Agent Verification

To verify that the Agent is running on a host, use one of the following procedures:

In the Connector Appliance or Logger GUI, click **Setup > System Admin > Process Status.** The ArcSight Management Center Agent (`arcmcagent`) will be shown as a process in the running state.

Verifying the Agent is Running For Software Connector Appliance or Software Logger (only)

After you install the Agent, at the command line, run this command at the command line:

```
<install_dir>/current/arcsight/<conapp|logger>/bin/<conappd|loggerd> status
```

The Agent is shown as a service in the running state.

Alternatively, in the Software Connector Appliance or Software Logger GUI, click **Setup > System Admin > Process Status.** The ArcSight Management Center Agent (`arcmcagent`) is shown as a process in the running state.

Uninstalling the ArcSight Management Center Agent.

- Always uninstall a previous version of the ArcSight Management Center Agent before installing a new version.
- If uninstalling either Software Logger or Software Connector Appliance, make sure that the ArcSight Management Center Agent is uninstalled from the node before beginning the uninstall of either product.

To uninstall the ArcSight Management Center Agent, run the following command:

```
<install_dir>/arcmcagent/UninstallerData/Uninstall_ArcSight_Management_Center_Agent_1.0
```

The Uninstall Wizard will launch. Click **Uninstall** to begin the wizard. When the uninstallation completes, click **Done**.

Chapter 3

The User Interface

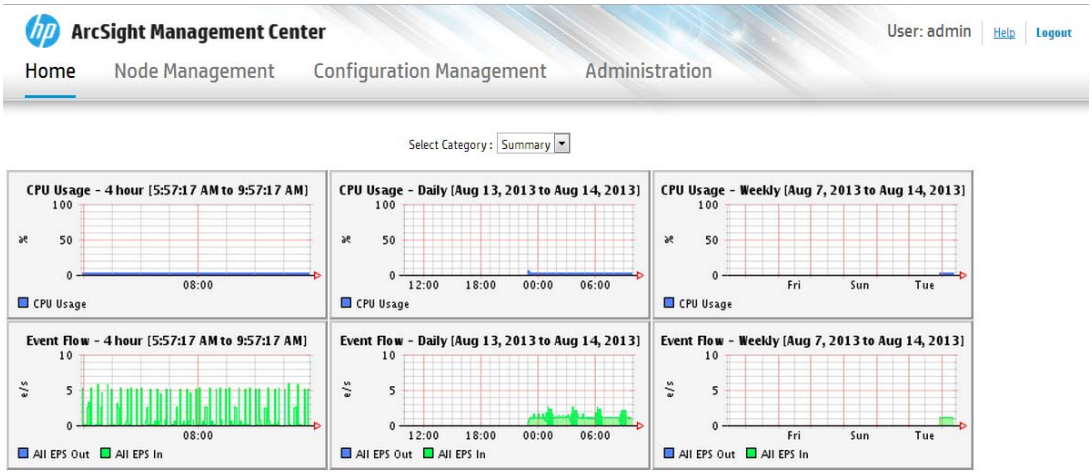
The following topics are discussed here.

Overview

This chapter provides a general overview of the ArcSight Management Center interface. ArcSight Management Center uses a browser-based user interface. Refer to the ArcSight Management Center Release Notes for the latest information on supported browsers.

The Menu Bar

The menu bar provides access to the main functional components of ArcSight Management Center. The menu bar includes the **Home**, **Node Management, Configuration Management a**nd **Administration** menus.



Home

The **Home** menu displays graphs of recent and current system performance.

- **Summary** shows CPU usage and event flow on four-hour, daily, and weekly scales.
- **Platform** shows CPU usage, platform memory usage, receive, transmit, disk read, and disk write values for selectable time periods: four hours, daily, or weekly.
- **Network** displays a graph for each networked host. The graph displays the bytes transmitted, overlaid on the bytes received for selectable time periods: four hour, daily, or weekly.

For more information on viewing monitoring graphs, see Chapter 4, Monitoring, on page 33.

Node Management

Use **Node Management** to manage any of the following node types:

- Software Connectors
- Connector Appliances
- Software Connector Appliances
- Loggers
- Software Loggers

For more information on adding and managing nodes, see Chapter 5, Managing Nodes, on page 37. From the same menu, you can also perform selected management tasks on managed ArcSight products. See Chapter 6, Managing HP ArcSight Products, on page 57.

Configuration Management

Use **Configuration Management** to create and manage node configurations, and synchronization (pushing) of configurations across multiple nodes. You can manage any of these configuration types:

- Logger configurations
- System Admin configurations
- Connector configurations
- Connector Appliance configurations

For more information on configuration management, see Chapter 7, Managing Configurations, on page 95.

Administration

The **Administration** menu contains these items:

- **Backup** enables you to back up your current ArcSight Management Center configuration. **Restore** enables you to restore your configuration from a saved backup. For more information, see Chapter 8, Managing Backups and Restores, on page 117.
- **Snapshot** enables you to take a snapshot image of HP ArcSight Management Center, to produce logs that are useful in troubleshooting. For more information, see Chapter 9, Creating Snapshots, on page 121.
- **Repositories** enables you to manage repositories that store files, such as logs, certificates, and drivers. For more information, see Chapter 10, Managing Repositories, on page 123.
- **System Admin** describes the system administration tools that enable you to create and manage users and user groups, and to configure security settings for your system.

For more information, see Chapter 11, System Admin - ArcSight Management Center, on page 139.

Help

Click the **Help** link to display the online help , which explains the functionality and features of ArcSight Management Center. From the help landing page, you can navigate to or search for specific topics.

About

The **About** screen displays the currently running version number of ArcSight Management Center. When done viewing, click **OK**.

Logout

Click **Logout** to end your ArcSight Management Center session.

By default, ArcSight Management Center automatically ends your session after 15 minutes of inactivity.

Chapter 4

Monitoring

The following topics are discussed here.

Overview

The **Home** tab displays the real-time and historical status of platform- and network-specific aspects of ArcSight Management Center, such as CPU, event flow, and disk usage statistics.

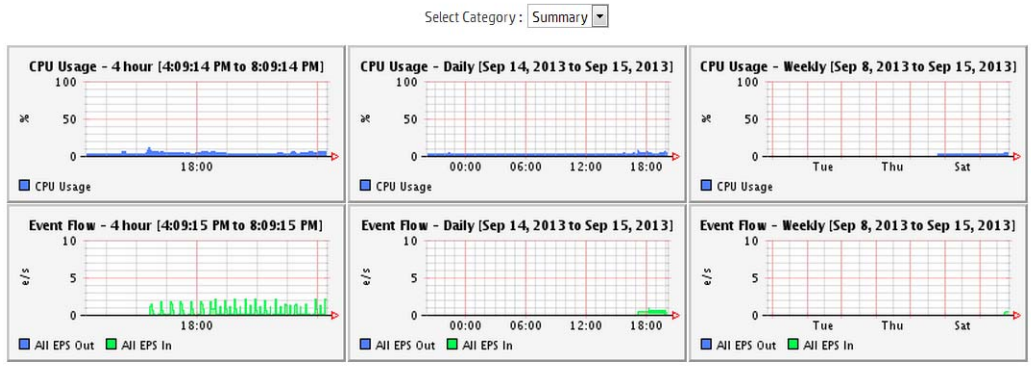
On the **Home** tab, you can select monitor displays for Summary, Platform, or Network. The Platform and Network monitor pages include a duration control. You can choose 4-hour, daily, or weekly time spans for historical data:

To select a monitor display,

1. On the **Home** page, under **Select Category**, select the monitor category from the drop-down list.
2. From the **Duration** drop-down list, select an interval for the data to be monitored. The corresponding graphs are displayed.]

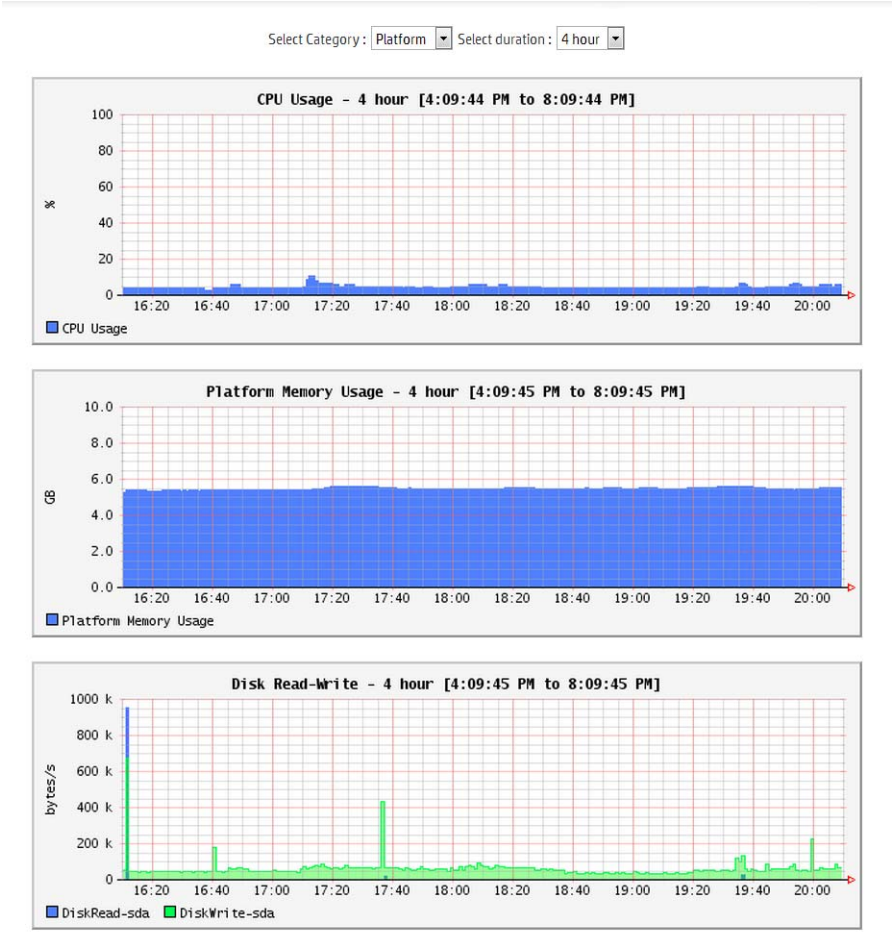
Viewing the Summary Page

The **Summary** monitor page displays graphs for each duration for CPU usage and event flow.



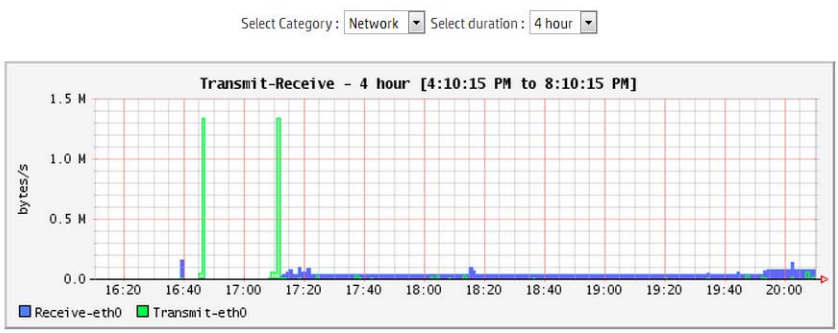
Viewing the Platform Page

The **Platform** monitor page displays information about CPU usage, memory usage, bytes received and sent on the network, and raw disk reads and writes.



Viewing the Network Page

The **Network** monitor page displays a graph for each network interface card. (The number of network interface cards varies by hardware model.) The graph displays the bytes transmitted, overlaid on the bytes received.



Chapter 5

Managing Nodes

The following topics are discussed here.

Overview

Node Management enables you to configure and organize nodes. A *node* is a networked ArcSight appliance or software application that can be centrally managed using ArcSight Management Center. Each node is associated with a single networked host which has been assigned a hostname, IP address, or both.

Node types can include software connectors, Connector Appliances, Software Connector Appliances, containers, Loggers, and Software Loggers.

A single host can include multiple nodes, and a node can be in a parent or child relationship to other nodes. For example, for a Connector Appliance with multiple containers, a single host, the Connector Appliance would be the parent node and each container a child of the parent node.

You can perform any of the following node management tasks:

- View the entire system, or view managed nodes by location, by host, or by node type.
- Add, view, edit, and delete locations for hosts.
- Add nodes from a host, import connector hosts, view and delete hosts, view all hosts in a location, move hosts to different locations, scan hosts for new connectors or containers.

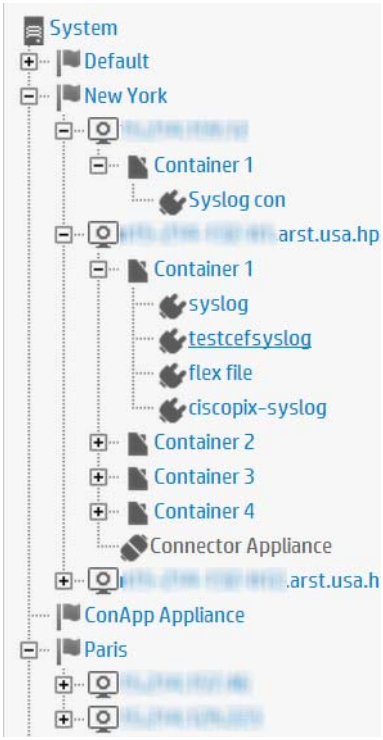
Node Management

To manage nodes, on the menu bar, click **Node Management.** The Node Management UI displays, as shown here.

The Node Management UI comprises two panels:

- The left side displays the navigation tree.
- The right side displays the Management panel, enabling you to perform management operations on items selected in the navigation tree.

The Navigation Tree



The navigation tree organizes managed nodes into a hierarchy, and comprises the following:

System: System displays the entire set of nodes managed by ArcSight Management Center.

Locations: Individual locations are displayed under **System**, listed in the order in which they were added. Locations are logical groupings you can use to organize a list of hosts. For more information, see "Locations" on page 47.

Hosts: Each location branch shows all hosts assigned to that location, listed by hostname, in the order in which they were added. For more information, see "Hosts" on page 49.

Nodes: Each host branch shows all managed nodes associated with that host. A node could be any of the following types:

Connector Appliance or Software Connector Appliance: Each Connector Appliance or Software Connector Appliance is shown as a separate node.


Logger Appliance or Software Logger: Each Logger Appliance or Software Logger is shown as a separate node.


Container: A container on a host, if any, is shown as a node.


Connector: If a container node contains a connector, the connector is shown under the container node in which it is contained.

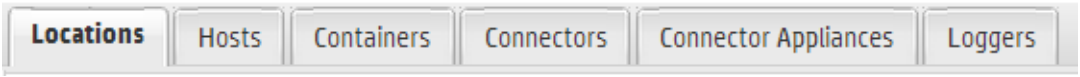
To view the number of nodes associated with a host, hover over the host entry in the tree. The count shown includes the host itself.

Since items in the tree are organized hierarchically, each item in the tree includes all branches displayed below it. For example, a **Location** branch includes all hosts assigned to that location. Click **+** to expand any branch and view any items included in the branch.

The Management Panel

Select an item in the navigation tree to display its details on one of the tabs in the Management panel. For example, to display the details of a host shown in the navigation tree, select the host in the tree. The Management panel will display details and controls pertaining to that host.

Management Tabs



The tabs displayed in the management panel depend on the type of item selected in the navigation tree

Selected Item Type	Management Tabs Shown
System	**Locations, Hosts, Containers, Connectors, Connector Appliances, Loggers**
Location	**Hosts, Containers, Connectors, Connector Appliances, Loggers**
Host	**Containers, Connectors, Connector Appliances, Loggers**
Node	**Connectors, Connector Appliances, Loggers**

For example, if you selected a location item from the navigation tree, the **Hosts, Containers**, **Connectors, Connector Appliances**, and **Logger** tabs would be shown. Each tab would display the items of the named type associated with the selected location, including details on those items. For example, the **Hosts** tab would show any hosts in the location, while the **Connector Appliances** tab would show any Connector Appliances in the same location.

Tab Controls

These controls are commonly displayed on all tabs in the Management panel:

- **Toolbar Buttons:** Toolbar buttons enable operations related to the items on the tab.
- **Items List:** Items corresponding to the tab header are displayed in a list. For example, locations are listed on the **Locations** tab.
- **Table Header Check Box:** Click the check box in the table header to toggle selection of all check boxes in a single column.
- **Bulk Operations Buttons:** On most tabs, buttons beneath the items list enable you to perform operations on one or more items. Choose one or multiple items in the list by selecting the checkbox next to each, and then click the button to perform the indicated operation. For example, to delete multiple items such as hosts, select one or more hosts on the **Hosts** tab, and then click **Delete**. The selected hosts would be deleted.

In addition, each tab may have controls individual to that item type. For example, the **Connectors** tab includes controls related to the management of connectors (see Chapter 6, Managing Connectors, on page 71).

The Locations Tab

The **Locations** tab displays all locations defined in ArcSight Management Center.

The **Locations** tab includes these buttons:

Add Location	Adds a new location.
Import	Imports connector host information from a CSV file.
Refresh	Refreshes tab data.
Filter	Displays drop down lists of values on which to filter each table column.

The **Locations** tab includes the following columns:

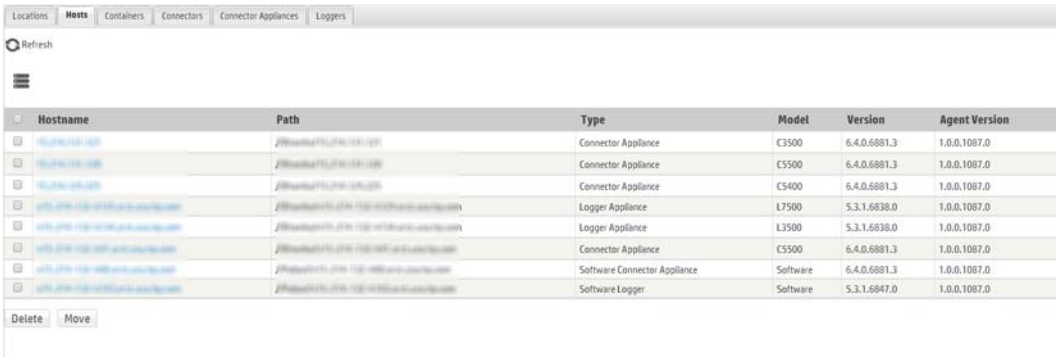
- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.
- **Action:** Shows a control for editing a location. For more information on editing a location, see "Editing a Location" on page 48.

This button enables operations on one or more selected locations:

- **Delete**: Deletes the selected locations from ArcSight Management Center.

For more information on managing locations, see “Locations” on page 47.

The Hosts Tab



The **Hosts** tab displays all hosts associated with the location selected in the navigation tree.

The Hosts tab includes these buttons:

Add Host	Adds a host.
Edit	Edits a host.
Refresh	Refreshes tab data.
Filter	Displays drop down lists of values on which to filter each table column.

The **Hosts** tab includes the following columns:

- **Hostname:** Fully qualified name of the host.

> **Note** This hostname must match the hostname in the host’s SSL certificate. If they do not match, such as when the certificate has been regenerated, the label Host Certificate Mismatch will be displayed.

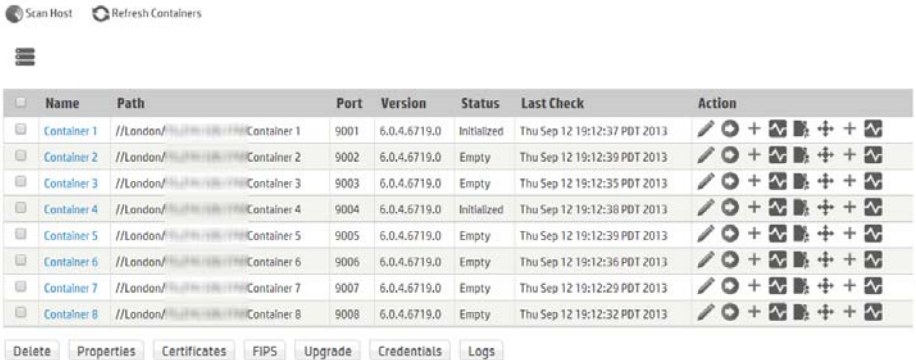
- **Path**: Path to the host.
- **Type**: Type of host.
- **Model**: If an appliance, shows the HP ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.
- **Version**: Version number of the software on the host.
- **Comment:** Any comments on the host.
- **Action:** Shows a control for scanning a host for new connectors. For more information on scanning a host, see Chapter 6, Managing Connectors, on page 71.

These buttons enable operations on one or more selected hosts:

- **Delete**: Deletes the selected hosts from ArcSight Management Center.
- **Move:** Moves the selected hosts to a new location.

For more information on managing hosts, see “Hosts” on page 49.

The Containers Tab



The **Containers** tab displays all containers associated with the item selected in the navigation tree. For example, if you selected a location in the tree, since locations include hosts, the **Containers** tab would display all containers associated with all hosts in the selected location.

The **Containers** tab includes these buttons:

Scan Host	Scans a host.
Refresh	Refreshes tab data.
Filter	Displays drop down lists of values on which to filter each table column.

The **Containers** tab includes the following columns:

- **Name:** Name of the container.
- **Path**: Path to the container.
- **Port**: Port number through which the container is communicating.
- **Version**: Software version of the container.
- **Status**: Status of the container.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing container management tasks. These enable editing of containers, sending commands to containers, adding a new connector to a container, running Logfu diagnostics, displaying a list of container certificates, deploying a container, starting the FlexConnector wizard, and starting the Diagnostics wizard. These controls are explained in detail in Chapter 6, Managing Containers, on page 62.

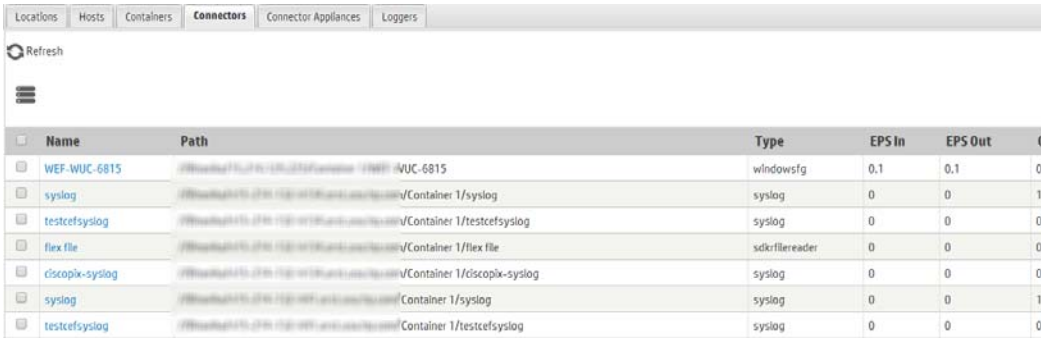
These buttons enable operations on one or more selected containers.

- **Delete**: Deletes the selected containers from ArcSight Management Center.
- **Properties:** Set properties on selected containers.
- **Certificates:** Manage certificates on selected containers.
- **FIPS:** Enable or disable FIPS on selected containers.

- **Upgrade:** Upgrades selected containers.
- **Credentials:** Manage credentials on selected containers.
- **Logs:** Manage logs on selected containers.

For more information on managing containers, see Chapter 6, Managing Connectors, on page 71.

The Connectors Tab



The **Connectors** tab displays all software connectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Connectors** tab would show all connectors in the selected container.

If the selected item in the navigation tree is a container, a toolbar enables connector and container management tasks, including adding a new connector, editing the container, sending container commands, running Logfu diagnostics, refreshing the list of connectors, displaying a list of container certificates, deploying a container, starting the FlexConnector wizard, and starting the Diagnostics wizard. For details of each of these tasks, see Chapter 6, Managing Connectors, on page 71.

The **Connectors** tab includes these buttons:

Refresh	Refreshes tab data.
Filter	Displays drop down lists of values on which to filter each table column.

The **Connectors** tab includes the following columns:

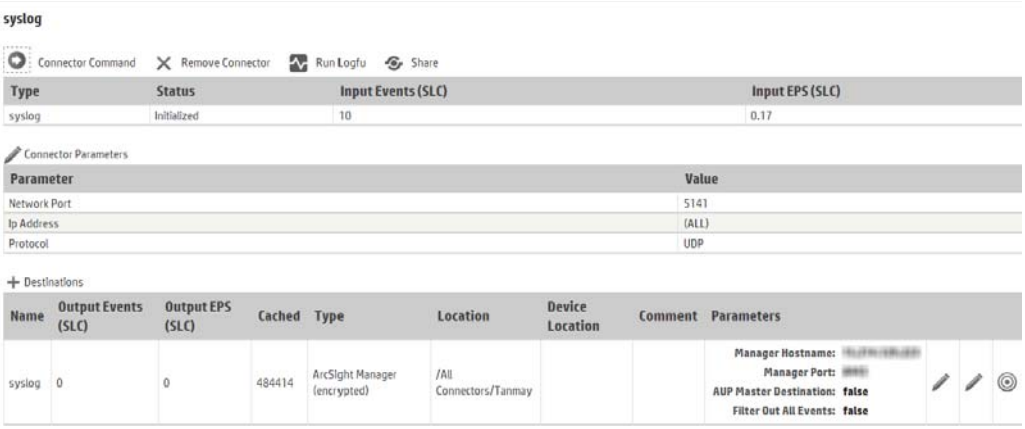
- **Name:** Name of the connector.
- **Path:** Path to the connector.
- **Type:** Type of connector.
- **EPS In:** Events per second received by the connector.
- **EPS Out:** Events per second sent by the connector to its destination.
- **Cache:** Connector cache size.
- **Last Check:** Date and time of the last status check.
- **Action:** Shows a variety of controls for executing software connector management tasks. These enable sending a connector command, sharing a connector, and starting the FlexConnector edit wizard.

These buttons enable operations on one or more selected connectors.

- **Delete**: Deletes connectors from ArcSight Management Center.
- **Runtime Parameters:** Change the runtime parameters on selected connectors.
- **Destinations:** Sets the destinations of selected connectors.
- **Parameters:** Sets the parameters of selected connectors.

For more information on managing connectors, see Chapter 6, Managing Connectors, on page 71.

The Connector Summary Tab



To view a single connector in detail, click the connector in the navigation tree.

The toolbar on the summary tab includes the following buttons:

Send Command	Sends a command to the connector.
Remove Connector	Removes the connector.
Logfu	Run Logfu diagnostics on the connector.
Share Connector	Shares the connector through ArcExchange.

Tables below the toolbar show connector specifics, including basic connector data, parameters, and connector destinations. These tables include the following columns:

Connector Data

- **Type:** Type of connector.
- **Status:** Connector status. Possible values for status are:
  - *Improper configuration:* Initial default state.
  - *Initializing connection:* The connector has a URL, but ArcSight Management Center has not logged in.
  - *Down*: There was an exception trying execute the login command.
  - *Unauthorized:* The login command was executed but failed.

- *Connecting:* Login in progress.
- *Connected:* Login completed successfully.
- *Empty:* Login completed successfully, but the container doesn't have connectors.
- *Initialized:* Login completed successfully and the container has connectors.

- **Input Events (SLC):** Total number of events received by the connector since it was last checked (generally once per minute).
- **Input EPS (SLC):** Events per second received by the connector since it was last checked (generally once per minute).

Connector Parameters

Click **Connector Parameters** to toggle display of this table. **Connector Parameters** includes:

-  Click to edit parameters.
- **Parameters:** Parameters include connector network port, IP address, and protocol.
- **Value:** Parameter value.

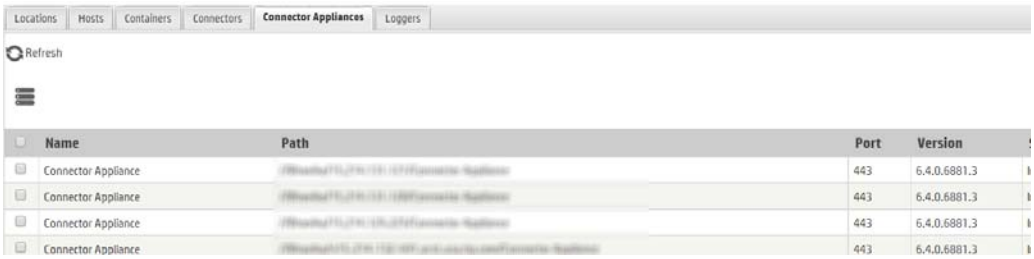
Destinations

Click **Destinations** to toggle display of this table. **Destinations** includes:

-  Click to enable additional destinations.
- **Name:** Destination name.
- **Output Events (SLC):** Total number of events output by the connector to the destination since it was last checked (generally once per minute).
- **Output EPS (SLC):** Events per second output by the connector to the destination since it was last checked (generally once per minute).
- **Cached:** Total number of events cached to be transmitted to the destination.
- **Type:** Destination type.
- **Location:** Location of the destination.
- **Device Location:** Location of the device on which the destination is located.
- **Comment:** Comments on the destination.
- **Parameters:** Destination-specific parameters, such as IP address, port, and protocol.
- **Action Buttons:** Action buttons enable destination management tasks, such as editing the destination, removing the destination, editing the runtime parameters, adding a new failover destination, and sending destination commands.

For more information on managing connectors, see Chapter 6, Managing Connectors, on page 71.

The Connector Appliances Tab



The **Connector Appliances** tab displays all hardware and Software Connector Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Connector Appliances** tab would display all Connector Appliances in ArcSight Management Center; if you selected a Location, the tab would display all Connector Appliances in the selected location.

The **Connector Appliances** tab includes the following button:

Filter	Displays drop down lists of values on which to filter each table column.

The **Connector Appliances** tab includes the following columns:

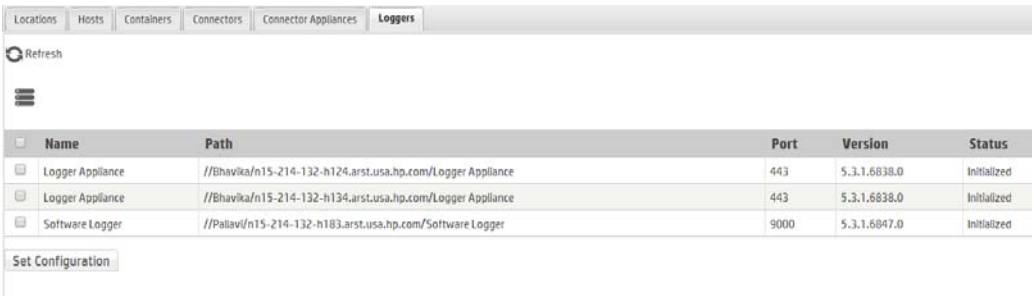
- **Name:** Name of the Connector Appliance.
- **Path**: Path to the Connector Appliance.
- **Port**: Port number through which the Connector Appliance is communicating.
- **Version**: Software version of the Connector Appliance.
- **Status**: Status of the Connector Appliance.
- **Last Check:** Date and time of last status check.
- **Action:** Shows a variety of controls for executing Connector Appliance management tasks, including rebooting, shutting down, and editing a configuration.

This button enable operations on one or more selected Connector Appliances.

- **Set Configuration:** Set the configuration of selected Connector Appliances.

For more information on managing Connector Appliances in ArcSight Management Center, see Chapter 6, Managing Connector Appliances, on page 57.

The Loggers Tab



The **Loggers** tab displays all hardware and Software Loggers associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree,

the **Loggers** tab would display all Loggers in ArcSight Management Center; while if you selected a Location, you would see all Loggers in that location.

The **Loggers** tab includes the following button:

 **Filter**	Displays drop down lists of values on which to filter each table column.

The **Loggers** tab includes the following columns:

- **Name:** Name of the Logger.
- **Path**: Path to the Logger.
- **Port**: Port number through which the Logger is communicating.
- **Version**: Software version of the Logger.
- **Status**: Status of the Logger.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing Logger management tasks, including rebooting, shutting down, and editing a configuration.

This button enable operations on one or more selected Loggers.

- **Set Configuration:** Set the configuration of selected Loggers.

For more information on managing Logger Appliances in ArcSight Management Center, see Chapter 6, Managing Loggers, on page 59.

Locations

A *location* is a logical grouping of hosts. The grouping can be based on any criteria you choose, such as geographical placement or organizational ownership. Locations are a useful way to organize hosts.

For example, you can group all hosts in New York separately from hosts in San Francisco and assign them the same location. Similarly, you can group hosts under “Sales” and others under “Marketing”.

A location can contain any number of hosts. For information on adding hosts to locations, see “About Adding Hosts” on page 49.

ArcSight Management Center includes one location by default (called *Default*) but you may add any number of others. The name of the Default location may be edited, if desired.

Adding a Location

You can add any number of locations.

To add a location:

1. Click **Node Management**.
2. In the navigation tree, click **System**.

3 In the management panel, click +.

4 Enter the name of the new location, and then click **Next**.

5 Click **Done**. The new location is shown in the System tree.

Editing a Location

You can edit the name of a location.

To edit a location:

1 Click **Node Management**.

2 In the navigation tree, click **System**, and then click the **Locations** tab.

3 On the **Locations** tab, choose one or more locations to rename by selecting the checkbox next to each.

4 Under **Action**, click  .

5 Enter the new name of each location, and then click **Next**.

6 Click **Done**. The location is renamed.

Viewing All Locations

You can see all the locations that exist in ArcSight Management Center.

To view all locations:

1 Click **Node Management**.

2 In the navigation tree, click **System**, and then click the **Locations** tab to view all locations.

Deleting a Location

When you delete a location from ArcSight Management Center, any hosts (and their associated nodes) are also deleted.

If you want to remove the location but still want to keep its hosts in ArcSight Management Center, relocate the hosts before deleting the location. See "Moving a Host to a Different Location" on page 53.

To delete a location:

1 Click **Node Management**.

2 In the navigation tree, click **System**, and then click the **Locations** tab.

3 On the **Locations** tab, choose one or more locations to delete by selecting the checkbox next to each.

4 Click **Delete**.

5 Click **OK** to confirm deletion. The selected locations are deleted.

Hosts

A *host* is a networked system associated with a unique IP address or hostname. A host can be an ArcSight appliance, or a system running an ArcSight software product, such as Software Logger.

About Adding Hosts

After a host is added to ArcSight Management Center, ArcSight products on the host becomes *nodes,* and can be managed. For example, adding a system hosting Connector Appliance with 4 containers would add 5 nodes to ArcSight Management Center: the Connector Appliance itself, and each container.

Prerequisites for Adding a Host

Ensure that these prerequisites are met before adding a host to ArcSight Management Center.

- **Host or Connector Credentials/Port:** You will need the username and password required for logging in to the software application or appliance to be added as a host. The following table shows the required information for each host type:

Table 5-1 Required Information for Adding a Host

Host Type	Required Information
Connector Appliance or L3xxx	• Host Credentials • Connector Credentials
Logger Appliance	• Host Credentials
Software Connector Appliance or Software Logger	• Host Credentials • Port
Software Connector	• Connector Credentials • Port

- **An SSL Certificate:** An SSL certificate must be generated for any Connector Appliance, Software Connector Appliance, Logger, or Software Logger to be managed. The hostname of the certificate must match the hostname you will add to ArcSight Management Center. For more information on generating certificates for these host types, consult the HP ArcSight Administrator's Guide for each product. (If a host to be added already has a certificate installed, you can use the existing certificate, as long as the hostname on the certificate matches the hostname of the host you will be adding.)
- ArcSight Management Center **Agent Installation (Software Connector Appliance or Software Logger Only):** Prior to adding a Software Connector Appliance or Software Logger host to ArcSight Management Center, confirm that the ArcSight Management Center Agent is installed and running on the host to be added. For more

information on installing the ArcSight Management Center Agent, see "Installing the ArcSight Management Center Agent" on page 26.

Note

On Loggers and Connector Appliances, the ArcSight Management Center Agent must be running in order for the host to be added to ArcSight Management Center, and will be started automatically after installation. However, in some cases, the ArcSight Management Center Agent may fail to start automatically and must be started manually. For information on starting the ArcSight Management Center Agent manually, see "Starting, Stopping, or Restarting the Agent" on page 27.

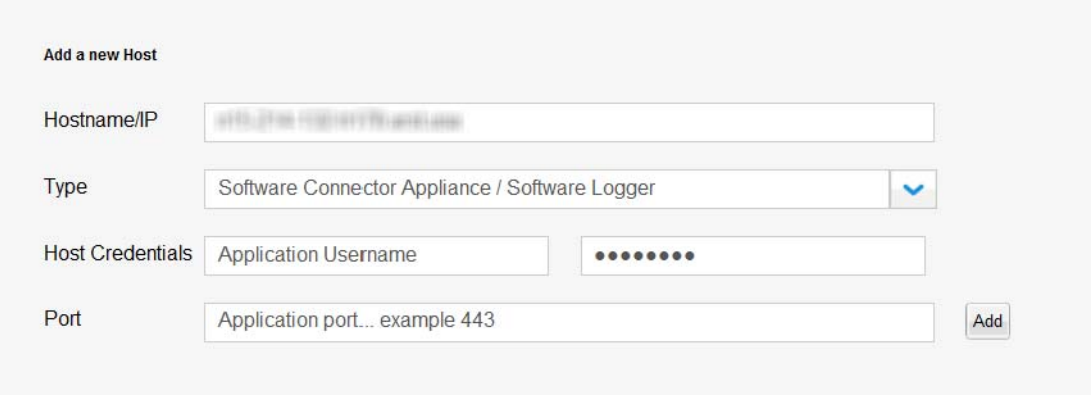
Limitations on Adding a Host

Adding a host has these limitations:

- **Only One Node Per Host:** In general, running more than one ArcSight software application on the same physical host (for example, both Software Logger and Software Connector Appliance) is not recommended. If a physical host is running more than one ArcSight software application, only one of these applications may be added as a node to ArcSight Management Center. This restriction does not apply to software connectors.
- **Client Authentication/Local Password Not Supported:** A host with client authentication and a local password enabled cannot be added to ArcSight Management Center.
- **FIPS Mode Not Supported:** Neither a Connector Appliance nor a Logger can be added as a host if in FIPS mode. This applies to both hardware and software form factors.

Adding a Host

You can add a software connector, Connector Appliance (software or hardware), or Logger (software or hardware) as a host.



To add a host:

1. Click **Node Management**.
2. In the navigation tree, select a location to which you plan to add the host.
3. On the **Hosts** tab, click **Add Host.**

4 On the **Add a new Host** dialog, in **Hostname/IP,** enter either the hostname or IP address of the host.

Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address.

If hostname is used, the hostname entered must match the hostname from the host's SSL certificate.

5 In **Type,** select the type of node from the drop-down list.

6 Enter values for the required settings. (Required settings will depend on the node type, as shown in Table 5-1 on page 49.

- In **Host Credentials** or **Connector Credentials**, enter the username and password required for authentication. (If the host is configured for external authentication, such as for LDAP or RADIUS, supply the external authentication credentials.)
- In **Port**, if required, enter the value of the port on which ArcSight Management Center will connect to the host.

7 Click **Add**. The host is added to ArcSight Management Center.

Adding a Host with Containers

When you add a host that includes containers (such as Connector Appliance), ArcSight Management Center also attempts to retrieve the SSL certificates from any containers that reside on the host, and add each container as a separate node. Containers on the remote host can be managed only if the system can authenticate using the certificates and supplied credentials. When the certificates are retrieved, you are prompted to import them into ArcSight Management Center.

Importing Connector or Container Hosts

To add connector (or container) hosts in bulk, you can import a comma-separated values (CSV) file with data on the connectors or containers to be added. When you add a host, the containers (and connectors) on the system are scanned automatically, and the CA certificates from the containers that reside on the host are retrieved. You can manage the containers on the hosts only if it can authenticate using the certificates and the supplied credentials. When the certificates are retrieved, you are prompted to import them.

CSV File Format

The header line of the file must consist of the following comma-separated keywords:

```
location,hostname,<starting port number for connector
scan>,type,username,password
```

Each subsequent line in the file represents a separate host and must include values for each of the keywords in the header line. For example,

```
East,hostname.example.com,9001,Software Connector,connector_user,
change_me
```

Also, if the file was created on a Windows system, ensure that an end-of-line character is included in the last line of the CSV file.

To import connector hosts from a CSV file:

1 Click **Node Management**.

2 In the navigation tree, click **System**.

3 In the management panel, click the **Locations** tab.

4 On the **Locations** tab, click  . The Import Connector Hosts wizard starts.

5 Select **Remote hosts (CSV format),** and then click **Next**. Follow the instructions in the wizard to upload the file.

6 Connector certificates are retrieved automatically so that the system can communicate with each connector in a container. The Upload CSV wizard lists the certificates. (To see certificate details, hover over the certificate.)

- Select **Import the certificates...**, and then click **Next** to import the certificates and continue.
- Select **Do not import the certificates...**, and then click **Next** if you do not want to import the certificates. The Upload CSV wizard does not complete the upload CSV process.

The Upload CSV wizard does not complete the upload if certificate download failed for any of the connectors in a container or if any of the certificates failed to import into the trust store on the system.

Viewing All Hosts

You can see all the hosts managed by ArcSight Management Center, or view them by location.

To view all hosts:

1 Click **Node Management**.

2 In the navigation tree, click **System**. (To view by location, click the location you wish to view.)

3 Click the **Hosts** tab. All managed hosts are displayed.

Viewing Managed Nodes on a Host

You can see all the managed nodes that exist on a host.

To view managed nodes on a host:

1 Click **Node Management**.

2 In the navigation tree, click the location to which the host is assigned. Then, click the host.

3 Click the appropriate tab to view the nodes for the host: **Containers, Connectors**, or **Connector Appliances,** or **Loggers**

Deleting a Host

When you delete a host, any nodes associated with the host are also deleted. Deleting a host removes its entry from ArcSight Management Center, but otherwise leaves the host machine unaffected.

To delete a host:

1 Click **Node Management**.

2 In the navigation tree, click **System**, and then click the **Hosts** tab**.**

3 Choose one or more hosts to delete by selecting the checkbox next to each.

4 Click **Delete**.

5 Click **Yes** to confirm deletion. The host (and any associated nodes) are deleted.

Moving a Host to a Different Location

You can assign one or more hosts to a new location. When you move a host, any nodes associated with it are also moved.

To move a host:

1 Click **Node Management**.

2 In the navigation tree, click **System**, and then click the **Hosts** tab**.**

3 Choose one or more hosts to move by selecting the checkbox next to each.

4 Click **Move**.

5 Follow the prompts in the **Host Move** wizard.The selected hosts are reassigned to their new locations.

Scanning a Host

Scanning a host will inventory all containers on the host and retrieve any CA certificates from each container. You should scan a managed host whenever you add connectors to (or remove connectors from) a host, to ensure ArcSight Management Center has an up-to-date connector count. You can scan these host types: Connector Appliance, Logger (L3X only), or software connectors.

A host is scanned automatically when first added to ArcSight Management Center.

When you scan a host, the CA certificates from the containers that reside on the host are retrieved. The containers on the remote host can be managed only if ArcSight Management Center can authenticate using the certificates and the credentials. When the certificates are retrieved, you are prompted to import them into the trust store.

A host scan will fail if any of the following are true:

- Any containers on a scanned Connector Appliance host are down.
- If you choose *not* to import the certificates that are retrieved.
- Authentication fails on any of the containers.

To scan a host:

1 Click **Node Management**.

2 In the navigation tree, select the location to which the host has been assigned.

3 Click the **Hosts** tab.

4 In the **Action** column for the host to be scanned, click  . The Host Scan wizard starts.

5 Click **Next** in the Host Scan wizard.

6 Enter values for the parameters in the following table, and then click **Next**.

Parameter	Description
Starting Port	The port number on the host on which ArcSight Management Center starts scanning for containers.
Ending Port	The port number on the host on which ArcSight Management Center ends scanning for containers.
User	The user name to authenticate with the host.
Password	The password for the user name you provide.

7 Connector certificates are retrieved automatically so that the ArcSight Management Center can communicate with each connector in a container. The Host Scan wizard lists the certificates. (To see certificate details, hover over the certificate.)

- To continue the scan, select **Import the certificates**, and then click **Next** to import the certificates and continue.
- Otherwise, select **Do not import the certificates,** and then click **Next**. The Host Scan wizard does not continue the scan.

Remote Connectors on Software Connector Appliance or Software Logger

When you add a Software Connector Appliance or Software Logger as a host, it is scanned automatically for the currently-running containers and the connectors associated with them. If additional containers are added to the remote host after it has been added to the system, you need to scan the host manually to detect the new containers. For information about scanning hosts, see "Scanning a Host" on page 53.

To manage these software connectors, you need to perform steps on the software connector that enable remote management.

To manage a remote connector:

1 Install the connector on the remote host as a service. Follow the instructions in the connector's configuration guide.

2 After completing the installation, open the file `/opt/arcsight/connectors/connector_x/current/user/agent/agent.properties` on the remote host and add these two properties:

```
remote.management.enabled=true

remote.management.listener.port=<9001>
```

The property `remote.management.enabled` configures the connector to be managed remotely. The property `remote.management.listener.port` specifies the port on which the connector receives commands from ArcSight Management Center.

- If port 9001 is already in use on the same host by another remotely managed connector or by any other application, change this value to any available port. You should use a port in the range 9001 - 9020.
- If you want to manage more than one software connector on the same host, you must specify sequential ports; for example, 9002, 9003, 9004.

3 Restart the connector service.

Continue by following the steps under “Adding a Host” on page 50.

Chapter 6

Managing HP ArcSight Products

The following topics are discussed here.

Overview

ArcSight Management Center enables management tasks on a variety of HP ArcSight products, including hardware and Software Connector Appliances, hardware and Software Loggers, containers, and software connectors. This chapter discusses the remote management of these products.

Managing Connector Appliances

You can perform any of the following management tasks on managed Connector Appliances or Software Connector Appliances using ArcSight Management Center.

- Reboot or shut down
- Edit or remove a configuration
- Set a configuration on one or multiple Connector Appliances

Not all Connector Appliance functionality is accessible through ArcSight Management Center. For a complete discussion of Connector Appliance features, see the Connector Appliance Administrator's Guide.

Rebooting

You can reboot a managed Connector Appliance.

To reboot a Connector Appliance:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, locate the Connector Appliance to be rebooted. In the **Action** column, click  .
5. Click **Next** to confirm reboot.
6. The Connector Appliance is rebooted. Click **Done**.

Shutting Down

You can shut down a managed Connector Appliance.

To reboot a Connector Appliance:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, locate the Connector Appliance to be shut down. In the **Action** column, click  .
5. Click **Next** to confirm shut down.
6. The Connector Appliance is shut down. Click **Done**.

Editing or Removing a Configuration

You can edit a configuration on, or remove property values of a list configuration from, a managed Connector Appliance.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, locate the desired Connector Appliance. In the **Action** column, click  . The Update Configurations wizard is launched.
5. Review the dialog box, and then click **Next**.
6. Follow the prompts to complete the wizard.

7 When the wizard is complete, click **Done**.

Setting a Configuration on Connector Appliances

You can set a configuration on one or multiple Connector Appliances using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Connector Appliances. Only new values will be appended. For example, if you had a set of users on three Connector Appliances, you could use Set Configuration to add the same new user to all of them. For more information on list configurations, see page 99.
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Connector Appliances.

Setting a configuration on one or multiple Connector Appliances may make each Connector Appliance node non-compliant with its current subscriptions.

To set a configuration on one or more Connector Appliances:

1 Click **Node Management**.

2 In the navigation tree, click **System**.

3 In the management panel, click **Connector Appliances**.

4 In the list of Connector Appliances, choose one or more Connector Appliances for which to set a configuration by selecting the checkbox next to each.

5 Click **Set Configuration**. The Set Configuration wizard is launched.

6 Review the dialog box, and then click **Next**.

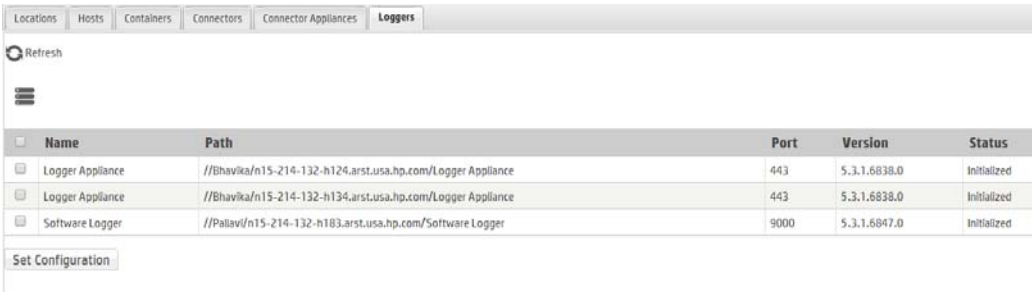
7 Follow the prompts to complete the wizard.

- Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.

8 The configuration is set on the selected Connector Appliances. Click **Done**.

Managing Loggers

You can perform any of the following management tasks on managed Logger Appliances or Software Loggers using ArcSight Management Center.



- Reboot or shut down
- Edit or remove a configuration

- Set a configuration on one or multiple Loggers

Not all Logger functionality is accessible through ArcSight Management Center. For a complete discussion of Logger features, see the Logger Administrator's Guide.

Rebooting

You can reboot a managed Logger.

To reboot a Logger:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the Logger to be rebooted. In the **Action** column, click  .
5. Click **Next** to confirm reboot.
6. The Logger is rebooted. Click **Done**.

Shutting Down

You can shut down a managed Logger.

To reboot a Logger:

1. Click **Node Management.**
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the Logger to be shut down. In the **Action** column, click  .
5. Click **Next** to confirm shut down.
6. The Logger is shut down. Click **Done**.

Editing or Removing a Configuration

You can edit a configuration on, or remove property values of a list configuration from, a managed Logger.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on a Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.

4 In the list of Connector Appliances, locate the desired Logger. In the **Action** column, click  . The Update Configurations wizard is launched.

5 Review the dialog box, and then click **Next**.

6 Follow the prompts to complete the wizard.

7 When the wizard is complete, click **Done**.

Setting a Configuration on Loggers

You can set a configuration on one or multiple Loggers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Loggers. Only new values will be appended. For example, if you had a set of users on three Loggers, you could use Set Configuration to add the same new user to all of them. For more information on list configurations, see page 99.
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Loggers.

Setting a configuration on one or multiple Loggers may make each Logger node non-compliant with its current subscriptions.

To set a configuration for one or more Loggers:

1 Click **Node Management**.

2 In the navigation tree, click **System**.

3 In the management panel, click **Loggers**.

4 In the list of Loggers, choose one or more Loggers for which to set a configuration by selecting the checkbox next to each.

5 Click **Set Configuration**. The Set Configuration wizard is launched.

6 Review the dialog box, and then click **Next**.

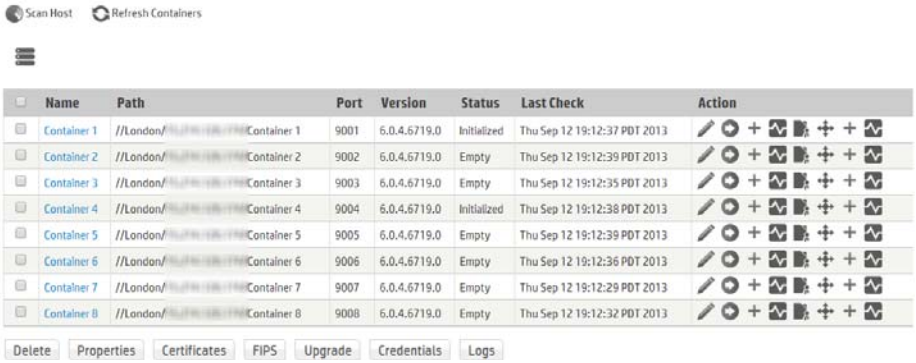
7 Follow the prompts to complete the wizard.

- Click **Add Row** to add a new Property to a list configuration, and then enter values as needed.

8 The configuration is set on the selected Loggers. Click **Done**.

Managing Containers

A *container* is a single Java Virtual Machine (JVM) that can run up to four connectors (This number depends on your current service agreement and the type of connector). Containers run on Connector Appliance and on Logger models L3XX.



A question mark (?) next to a container in the navigation tree indicates the connectors in the container cannot be authenticated. The CA certificates for the connectors might be no longer valid. Refer to "Resolving Invalid Certificate Errors" on page 70.

Viewing All Containers

You can view all containers managed in ArcSight Management Center.

To view all containers:

1. Click **Node Management**.
2. In the navigation tree, click **System**. (Alternatively, to view containers on a specific host, select the host from the navigation tree.)
3. Click the **Containers** tab to display the containers.

Viewing Connectors in a Container

You can see all the connectors in a container.

To view connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container whose connectors you wish to view.
3. Click the tree branch corresponding to the container.
4. Click the **Connectors** tab. The connectors in the container are displayed.

Editing a Container

The default name for a container is *Container N*, where N is a sequential number that indicates the order that the container was added. However, you can edit a container's default name.

To edit a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container you wish to rename.

3 On the **Connectors** tab, click  .

4 In **Name,** enter the new container name, field and then click **Next**.

5 Click **Done**. The container is renamed.

Deleting a Container

You can only delete containers from hosts that *do not* have a fixed number of containers, such as Software Logger or Software Connector Appliance. When you delete a container, the connectors that it contains are also deleted.

To delete a container:

1 Click **Node Management**.

2 In the navigation tree, navigate to the host on which the container resides.

3 Click the **Containers** tab.

4 On the **Containers** tab, select one or more containers to delete.

5 Click **Delete**.

6 Click **OK** to confirm deletion. The selected containers are deleted.

Updating Container Properties

You can update existing container properties, delete them, or add new ones.

To update container properties:

1 Click **Node Management**.

2 In the navigation tree, navigate to the host on which the container resides.

3 Click the **Containers** tab.

4 On the **Containers** tab, select one or more containers to update.

5 Click **Properties**.

6 Follow the instructions in the wizard to update the container properties.

When a property is removed, it is still visible until the container is restarted.

Changing Container Credentials

Each container has a user name and password associated with it. (The default user name is `connector_user` and the default password is `change_me`.)

Change each container's credentials to a non-default value before deploying it to production.

To update container properties:

1 Click **Node Management**.

2 In the navigation tree, navigate to the host on which the container resides.

3 Click the **Containers** tab.

4 On the **Containers** tab, select one or more containers for which to change the credentials.

5 Click **Credentials**.

6 Follow the instructions in the wizard to update connector credentials.

Sending a Command to a Container

You can run commands on a container to configure memory settings, pull an OPSEC certificate, generate a key, or restart the container.

To run a command on a container:

1 Click **Node Management**.

2 In the navigation tree, navigate to the host on which the container resides.

3 Click the **Containers** tab.

4 In the **Action** column of the container, click  . The Send Command wizard starts.

5 From the drop-down list, select the command you want to send, and then click **Next**.

6 Enter appropriate values for the parameters and then click **Done**.

Upgrading a Container to a Specific Connector Version

You can upgrade all connectors in a container to a specific version. Empty containers may be upgraded from versions 5.1.2 or later.

After you upgrade a container, wait at least 15 minutes before upgrading it again.

To upgrade a container to a specific connector version:

1 If it does not already exist, upload a connector build AUP from the HP ArcSight Customer Support site to the AUP (Upgrade) repository.

2 Click **Node Management**.

3 In the navigation tree, navigate to the host on which the container resides.

4 Click the **Containers** tab.

5 On the **Containers** tab, select one or more containers to upgrade.

6 Click **Upgrade**.

7 Select the version to which you want to upgrade the selected containers, and then click **Next**.

On a slow network or when the system is under a particularly heavy load, the upgrade might be interrupted by a session timeout. To prevent this interruption, upload the `.aup` file to a higher-performance system, then push the result to the lower-performance system.

Viewing Container Logs

You can retrieve and view the log files for one or more containers. The log files are in `.zip` format.

Container logs must be uploaded to the Logs repository before they can be viewed. For instructions on how to upload logs, see Chapter 10, Uploading a File to the Logs Repository, on page 124.

To retrieve and view container logs:

1 Click **Node Management**.

2 In the navigation tree, navigate to the host on which the container resides.

3 Click the **Containers** tab.

4 On the **Containers** tab, select one or more containers for which to view logs.

5 Click **Logs**.

6 Click **Next** to begin the **Retrieve Container Logs** process. When complete, click **Done**.

7 Click **Administration** > **Repositories.**

8 In the left panel, click **Logs**.

9 In the management panel, click  to retrieve the log files (in `.zip` format) you want to view.

Deleting a Container Log

You can delete unneeded container logs as necessary.

To delete a container log file:

1 Click **Administration > Repositories.**

2 In the left panel, click **Logs**.

3 In the management panel, on the list of logs, click  next to the log file you want to delete.

4 Click **OK** to confirm deletion.

Adding a Connector to a Container

Each container may hold up to 4 connectors.

To add a connector to a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container to which you wish to add a connector.
3. On the **Connectors** tab, click ➕. The **Connector Setup** wizard starts.
4. Click **Next**, and then follow the prompts to set up the new connector.

Always change the default credentials of any new connector to non-default values. For more information, see "Changing Container Credentials" on page 63.

Running Logfu on a Container

The Logfu utility is a diagnostic tool that parses ArcSight logs to generate an interactive visual representation of the information contained within the logs. When event flow problems occur, it can be useful to have a visual representation of what happened over time.

To run Logfu on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select a container to run Logfu.
5. In the **Action** column, click  .
6. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
   - In the **Group** box, choose which type of data you would like to view. The **Group** box lists all connectors within the chosen container, plus many other types of data such as memory usage and transport rates.
   - Then, choose one of the Group box data points. Depending on which data point you chose, a list of fields appears in the Field box below.
   - Choose a field to view. A graphic chart appears in the Chart box, providing rate and time information. The key at the bottom of the Chart box defines the data points mapped in the chart.
   - To choose a different data point for analysis, click **Reset Data**.
7. When complete, close the display window.

Managing Certificates on a Container

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The Certificate Management wizard, available from the **Containers** tab, helps you add and remove certificates on a container. Using the wizard, you can:

- Add a certificate to a container.
- Add certificates in bulk, enabling multiple containers at once.
- Enable or disable a demo certificate on a container that is in non-FIPS mode only.

- Add a CA Certs file on a container that is in non-FIPS mode only.
- Remove a certificate from a container.

From the **Containers** tab and the **Connectors** tab, you can view details about the certificates applied to a container. See "Viewing Certificates on a Container" on page 70.

For information about resolving invalid certificates, see "Resolving Invalid Certificate Errors" on page 70.

Adding CA Certificates to a Container

You can add a single CA certificate to a container that is in FIPS mode or non-FIPS mode.

Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Hover over a container name to see the type of certificate applied to it. Click the  icon to display a list of the certificates available on the container.

Before you perform the following procedure, make sure the certificate you want to add is loaded in the CA Certs repository.

To add a single CA certificate to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to add certificates.
5. Click **Certificates**. The Certificate Management wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Add Certificate**, and then click **Next**.
8. Follow the instructions in the wizard to add the certificate.

   If a container is down or a connector is running an older build, the wizard reports errors in the progress bar and on the Summary page.

Removing CA Certificates from a Container

You can remove CA certificates from a container when they are no longer needed. When you remove a CA certificate, the certificate is removed from the container's trust store; but it is **not** deleted from the repository.

Use caution when deleting certificates. When you delete a certificate on a container but the connector destination is still using that certificate, the connector can no longer communicate with the destination.

To remove CA certificates from a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.

3 Click the **Containers** tab.

4 On the **Containers** tab, select one or more containers to which you wish to remove certificates.

5 Click **Certificates**. The **Certificate Management** wizard starts.

6 Review the dialog box, and then click **Next**.

7 Under **Choose an Action,** select **Remove certificate**, and then click **Next**.

8 Select one or more certificates from the certificate list, and then click **Next**. The certificates are removed from the list of certificates and no longer used. When you remove a certificate from a container in FIPS mode, the container restarts automatically.

9 The Certificate Management wizard displays the certificates that are removed successfully in a comma-separated list. Certificates that cannot be removed are shown in a comma-separated list together with a reason why the certificate removal failed.

Adding a CA Certs File to a Container

You can add a CA Certs file to any container that is in non-FIPS mode.

When you apply a CA Certs file, the entire trust store on the container is overwritten. All previously-added certificates are overwritten.

Before you follow the procedure below, make sure that the CA Certs file you want to add is loaded in the CA Certs repository.

To add a CA Certs file to a non-FIPS mode container:

1 Click **Node Management**.

2 In the navigation tree, click **System**.

3 Click the **Containers** tab.

4 On the **Containers** tab, Select one or more non-FIPS mode containers to which you wish to add a CA Certs file.

5 Click **Certificates**. The **Certificate Management** wizard starts.

6 Review the dialog box, and then click **Next**.

7 Under **Choose an Action,** select **CA Cert (Legacy)**.

8 Follow the instructions in the wizard.

After the CA Certs file has been added to a container, the container restarts automatically.

Enabling or Disabling a Demo Certificate on a Container

You can use the demo certificate on a container for testing purposes. By default, the demo certificate on a container is disabled. You can enable the demo certificate temporarily for testing purposes on a container that is non-FIPS mode.

Enable a *demo* certificate on a container in non-FIPS mode for testing purposes only. Using a demo certificate in a production environment is a serious security issue because the demo certificate is not unique.

To enable or disable a demo certificate on a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers for which you wish to enable or disable a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Demo CA (Legacy)**, and then click **Next**.
8. Follow the instructions in the Certificate Management wizard.

   After you add the demo certificate on a container, the container restarts automatically.

Adding Multiple Destination Certificates to a Container

You can add multiple destination certificates to a container that is in FIPS mode or non-FIPS mode.

Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Click the  icon to display a list of the certificates available on the container.

To apply multiple destination certificates to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, containers for which you wish to add multiple destination certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, and then click **Next**.
7. Under **Choose an Action**, select **Import destination certificates** to add a certificate.
8. Follow the instructions in the wizard.

Viewing Certificates on a Container

From the Containers tab or the Connectors tab, you can display a list of the CA certificates applied to a container and view the details for a particular certificate in the list.

- On the **Containers** tab, click the  icon in the **Action** column for the container whose certificates you want to view.
- On the **Connectors** tab, select the  icon at the top of the page.

The Certificate List wizard displays the certificates applied to a container. To see details about a certificate, select the certificate, and then click **Next** at the bottom of the page.

Resolving Invalid Certificate Errors

If no valid CA certificates exist for the connectors in the container, a question mark (?) is shown for the container. You can resolve this invalid certificate error as follows:

To resolve the invalid certificate error:

1. Select the container in the navigation tree.
2. Click the **Connectors** tab. The error message is displayed.
3. Click  to run the Certificate Download wizard.
4. Follow the instructions in the wizard to download and import the valid certificates.

Running Diagnostics on a Container

You can run diagnostics on a container.

Diagnostic tools are also provided under **Administration > System Admin**. For more information, see "Diagnostic Tools" on page 63.

To run diagnostics on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to run diagnostics.
5. In the **Action** column, click  . The Diagnostics wizard starts.
6. Select the action you want to take on the selected container:
   - Select **Edit a configuration file** to edit a file in the `user/agent` folder on the container with the extension `.properties`, `.csv`, or `.conf`.
   - Select **Edit a user file** to edit any file (except binary files, such as `.zip`, `.jar`, or `.exe`) in the `user/agent` folder on the container.

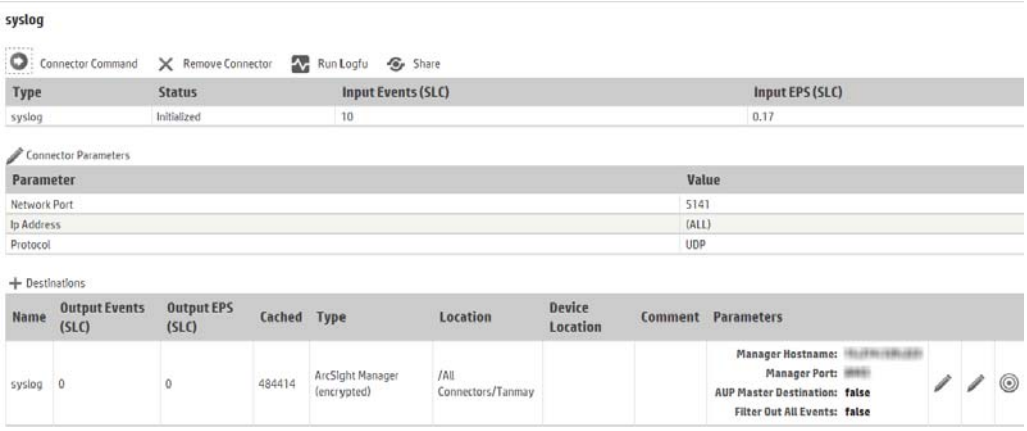
7 From the list of available files, select the file you want to edit. The file displays in the Edit File panel. Make your edits, and then click **Next** to save your edits and restart the container.

> **Note** When you click **Next**, ArcSight Management Center saves the updated file in the `user/agent` folder on the container. The original file is overwritten.

8 Click **Done** to close the Diagnostics wizard.

Managing Connectors

A *connector* (also known as a SmartConnector) is an HP ArcSight software component that collects events and logs from various sources on your network. A connector can be configured on ArcSight Management Center, on a Logger platform with an integrated Connector Appliance, or installed on a computer on your network, managed remotely. For a complete list of supported connectors, go to the HP ArcSight Customer Support site.



You can perform many operations on connectors. You can view all the connectors you are managing and add, remove, and edit a connector. You can update connector and table parameters, add and remove connector destinations, and edit destination parameters and runtime parameters. You can send a command to a connector or a destination. All these procedures are described below.

Viewing all Connectors

You can see all currently managed connectors.

To view all connectors:

1 Click **Node Management**.

2 Click **System** in the navigation tree.

3 In the management panel, click the **Connectors** tab. All connectors display on the Connectors tab in the management panel.

Adding a Connector

Prerequisites

Before you add a connector, review the following important information.

- Make sure that the container, host, and location to which you want to add the connector exist on the system. If any of these elements do not exist, first create them.
- Follow the configuration best practices described in "Configuration Suggestions for Connector Types" on page 90.

  If you are configuring the Check Point OPSEC NG Connector, see "Configuring the Check Point OPSEC NG Connector" on page 91 and refer to the SmartConnector Configuration Guide for Check Point OPSEC NG.

  If you are configuring a database connector that requires the MS SQL Server Driver for JDBC, follow instructions in "Adding the MS SQL Server JDBC Driver" on page 93.

This connector type has special requirements concerning JDBC and authentication setup. Refer to the SmartConnector Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB for this important information before installing the connector.

- If you are adding a software-based connector, make sure that the username and password for the connector match the username and password for the container to which you are adding the connector. Refer to "Changing Container Credentials" on page 63.
- For file-based FlexConnectors, make sure that an NFS Mount is established and a repository is created on the system before you add the connector. In addition, when entering the connector parameters, type the configuration file name without an extension in the Configuration File field. The extension `.sdkrfilereader.properties` is appended automatically.
- For detailed information about individual connector parameters, refer to the specific HP ArcSight SmartConnector Configuration Guide for the type of connector chosen. The configuration guide also describes how to set up the source device for use with the connector

To add a connector:

If you are adding a connector for the Check Point FW-1/VPN-1 system, see a more detailed procedure in "Configuring the Check Point OPSEC NG Connector" on page 91.

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the connector will reside.
3. In the management panel, click the **Containers** tab.
4. On the **Containers** tab, locate the container where you will assign the connector.
5. In the **Action** column of the container, click + . The Connector Setup wizard starts.
6. Review the dialog box, and then click **Next**.
7. Select a connector type from the pull-down list of available types, and then click **Next**.

8 Enter basic parameters for the connector. Parameters vary based on the connector type. (Hover over a field for more information on a field.) When all fields have been entered, click **Next**.

When entering parameters that include a file path, enter the path in POSIX format (for example, `/folder/filename`).

For file-based connectors on Windows systems, specify the name of the CIFS mount point you created for the connector. (You need to specify `/opt/mnt/CIFS_share_name`.)

Some connectors include table parameters. For example, the Microsoft Windows Event Log includes parameters for each host in the domain and one or more log types (security, application, system, directory service, DNS, file replication, and so on). You can import table parameters from a CSV file. You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

For connectors that query Microsoft Active Directory to detect devices (for example, Microsoft Windows Event Log - Unified), if the “Network Security: LDAP Server Signing Requirements” policy is set to “Signing Required” on the Domain Controller, ArcSight Management Center will be unable to connect to the Active Directory or browse for devices. You see an error when selecting **Windows Host Browser** as the connector device browser type.

9 Choose a primary destination for the connector and enter destination-specific parameters on the following page(s), and then click **Next**. Destinations can be:

- ArcSight Logger SmartMessage (encrypted)
- ArcSight Manager (encrypted)
- CEF Syslog (plaintext, that is, unencrypted)

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination,** and then click **Next** if you do not want to import the certificate. The destination will not be added.

10 Enter connector details:

Parameter	Description
Name	A descriptive name for this connector.
Location	The location of the connector (such as the hostname).
Device Location	The location of the device that sends events to the connector.

Parameter	Description
Comment	Additional comments.

11 When complete, click **Done**.

Editing Connector Parameters

HP ArcSight supports a large number of connector types to gather security events from a variety of sources, including syslog, log files, relational databases, and proprietary devices. Accordingly, configuration parameters vary widely depending on the type of connector being configured.

You can edit parameters (simple and table) for a specific connector, or for multiple connectors of the same type at the same time.

Updating Simple Parameters for a Connector

The following procedure describes how to update simple parameters for a specific connector.

To update parameters for a specific connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector you wish to update.

3 In the management panel, the **Connector** summary tab displays.

4 On the **Connector** tab, next to **Connector Parameters,** click  .

5 Modify parameters as necessary, and then click **Next**.

When editing parameters that include a file path, enter the path in POSIX format (for example, `/folder/filename`).

6 When complete, click **Done**. The updated parameters display in the **Connector Parameters** table of the Connector summary tab.

Updating Table Parameters for a Connector

Certain connectors, such as the Microsoft Windows Event connector, have table parameters. You can update the table parameters for a specific connector when necessary.

To update table parameters for a specific connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector you wish to update. In the management panel, the **Connector** summary tab displays.

3 On the **Connector** summary tab, next to **Table Parameters,** click  .

4 Modify parameters as necessary and then click **Next**.

- To add more rows of parameter information, click the **Add Row** link.

- You can use an Excel-compatible program to prepare a comma-separated values text file with the information and click the **Import File** button to load the entire table at once. The file needs to be in the same format as the rows shown on the Update Table Parameters page and needs to include a header row with parameter labels in the order shown on that page. For fields that require checkbox values, enter True or False as the value. An example is shown below.

	A	B	C	D	E	F
1	Domain Name	Host Name	User Name	Password	Security Logs	System Logs
2	test	1.1.1.1	admin	password	TRUE	FALSE
3	test2	1.1.1.1.1	admin	password	TRUE	FALSE

You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

5 When complete, click **Done**. The updated table parameters display in the Table Parameters section of the Connector page.

Updating Simple and Table Parameters for Multiple Connectors

If you have multiple connectors of the same type, you can change the simple and table parameters for all the connectors at the same time.

To edit parameters for multiple connectors of the same type:

1 Click **Node Management**.

2 In the navigation tree, select the host where the connectors reside.:

3 In the management panel, select the connectors whose parameters you want to update.

4 Click **Parameters**. The Update Connect Parameters wizard starts.

5 Review the dialog box, and then click **Next**.

6 Follow the instructions in the wizard.

- You can choose to modify the simple parameters for all the selected connectors at once or modify the simple parameters per connector.
- If the connectors have table parameters, the table parameters are displayed so that you can modify them. If you have many table parameters to modify for multiple connectors, you can import the parameters from a CSV file (for information about adding rows and CSV file format, see Step 4 on page 74). You can also export the table parameters to a CSV file for use as a backup or to import on another Connector Appliance.

When you update parameters for connectors of different versions, the newer connectors might have additional parameters. In this case, only those parameters shared by all connectors are displayed for updating.

7 Click **Done** when complete.

Managing Destinations

Connectors can forward events to more than one destination, such as ArcSight Manager and ArcSight Logger. You can assign one or more destinations per connector. You can assign multiple destinations to a connector and specify a failover (alternate) destination in the event that the primary destination fails.

The following procedures describe how to perform these actions on a specific connector or for multiple connectors at the same time:

- Add a primary or failover destination
- Edit destination parameters and destination runtime parameters
- Remove destinations
- Re-register destinations
- Manage alternate configurations for a destination
- Send a command to a destination

Adding a Primary Destination to a Connector

When you add a primary destination to a connector, you need to enter details for the destination, such as the destination hostname and port used.

To add a primary destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to connector to which you wish to add a destination.In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Destinations**, click ➕. The Add Destination wizard starts.
4. Follow the steps in the wizard. You can either select an existing destination or add a new destination. If you are adding a new destination, select the destination type and enter parameters for the destination.

For containers running 5.1.2.5823 and later, ArcSight Management Center retrieves the certificate for the ArcSight Manager destination automatically and displays the certificate summary.

For containers running 5.1.2 and earlier, upload the certificate on the container and then add the destination.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Failover Destination to a Connector

Each destination can have a failover destination that is used if the connection with the primary destination fails.

UDP connections cannot detect transmission failure; use Raw TCP for CEF Syslog destinations.

To add a failover destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click  . The Add Destination wizard starts.
4. Follow the steps in the wizard to select from available destinations and enter the destination details.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Primary or Failover Destination to Multiple Connectors

You can add a primary or failover destination to several connectors at the same time.

To add a primary or failover destination to multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click .
6. Review the dialog, and then click **Next**.
7. Under **Choose an Option**, select **Add a destination**, and then click **Next**.
8. Choose between a creating a new destination or selecting an existing destination, and then click **Next**.

- If you choose to **create a new destination**, select the destination type and then provide the destination parameters.
- If you choose to **select an existing destination**, select a destination from the list.

Note

ArcSight Management Center retrieves the ArcSight Manager certificate for the destination automatically and displays the certificate summary.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from destination**, and then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

9 Define the destination function by choosing between a primary or failover destination.

- If you choose **Primary destination**, click **Next** to update the configuration.
- If you choose **Failover destination**:
  - i Select the primary destination that applies to your failover.
  - ii Check the box in the table header to modify all of the displayed connectors.
  - iii Click **Next** to update the configuration.

10 Click **Done** when complete.

Removing Destinations

You can remove a destination from a connector at any time. Each connector must have at least one destination; as a result, you may not remove all destinations from a connector.

To remove a single destination from a connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector from which you wish to remove a destination. In the management panel, the **Connector** summary tab displays.

3 On the **Connector** summary tab, in the **Destinations** table, click ✕ for the destination you want to remove.

4 Click **OK** to confirm removal.

To remove multiple destinations from one or more connectors:

1 Click **Node Management**.

2 In the navigation tree, browse to the container where the connectors reside.

3 In the management panel, click the **Connectors** tab.

4 From the list of connectors, select all connectors to which you wish to assign a destination.

5 Click ✕.

6 Review the dialog, and then click **Next**.

7 Under **Choose an Option**, select **Remove a destination**, and then click **Next**.

8 Follow the instructions in the wizard, and click **Done** when complete.

Re-Registering Destinations

At certain times, you might need to re-register the destinations for one or more connectors; for example, after you upgrade ESM, or if a Logger appliance or ESM appliance becomes unresponsive.

To re-register destinations for one or more connectors:

1 Click **Node Management**.

2 In the navigation tree, browse to the container where the connectors reside.

3 In the management panel, click the **Connectors** tab.

4 From the list of connectors, select all connectors to which you wish to assign a destination.

5 Click **Destinations**.

6 Review the dialog, and then click **Next**.

7 Under **Choose an Option**, select **Re-register destinations,** and then click **Next**.

8 Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Parameters

The following procedures describe how to edit destination parameters for a specific connector and how to edit destination parameters for multiple connectors.

To edit destination parameters for a connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector to which you wish to edit destination parameters. In the management panel, the **Connector** summary tab displays.

3 In the **Destinations** table, click  next to the destination you want to edit to display the **Edit Destination Parameters** page.

4 Make your changes, and then click **Next**.

5 Click **Done** when complete.

To edit destination parameters for *multiple* connectors:

1 Click **Node Management**.

2 In the navigation tree, browse to the container where the connectors reside.

3 In the management panel, click the **Connectors** tab.

4 From the list of connectors, select all connectors for which you wish to edit destination parameters.

5 Click **Destinations.** The Manage Destinations wizard opens.

6 Review the dialog, and then click **Next**.

7 Under **Choose an Option**, select **Edit a destination**, and then click **Next**.

8 Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Runtime Parameters

The runtime parameters for a destination enable you to specify advanced processing options such as batching, time correction, and bandwidth control. The user interface automatically displays the parameters valid for a destination.

The following procedures describe how to edit the runtime parameters for a specific connector and how to edit the runtime parameters for multiple connectors at the same time.

To edit destination runtime parameters for *a* connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click next to the destination whose runtime parameters you want to edit.
4. Under **Add Alternate Configurations**, click  next to the alternate configuration that you want to edit.

   If you have not set up alternate configurations, click  next to the **Default**. For more information about alternate configurations, see "Managing Alternate Configurations" on page 80.
5. Specify or update values for the listed parameters, and then click **Save**.

To edit destination runtime parameters for *multiple* connectors at the same time:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination runtime parameters.
5. Click **Runtime Parameters** to open the wizard.
6. Follow these steps in the wizard to edit the runtime parameters:
   a. Select the destinations whose runtime parameters you want to modify.
   b. Select the configurations to be affected (default or alternate configurations).
   c. Select the group of parameters you want to modify (for example, batching, cache, network, processing).
   d. Modify the parameters.

Managing Alternate Configurations

An *alternate configuration* is a set of runtime parameters that is used instead of the default configuration during a specified portion of every day. For example, you might want to specify different batching schemes (by severity or size) for different times of a day. You can define more than one alternate configuration per destination, and apply them to the destination for different time ranges during the day. For example, you can define a

configuration for 8 a.m. to 5 p.m. time range and another configuration for the 5 p.m. to 8 a.m. time range.

By default, a configuration labeled **Default** is applied to a destination. Any subsequent configurations you define are labeled **Alternate#1**, **Alternate#2**, and so on. The default configuration is used if the time ranges specified for other alternate configurations do not span 24 hours. For example, if you specify an alternate configuration, **Alternate#1** that is effective from 7 a.m. to 8 p.m., the **Default** configuration is used from 8 p.m. to 7 a.m.

If you need to apply the same alternate configuration for multiple destinations, you need to define an alternate configuration (with the same settings) for each of those destinations.

Defining a New Alternate Configuration

The process of defining a new alternate configuration includes first defining the configuration, and then editing it to specify the time range for which that configuration is effective.

To define an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click  .
4. Under **Add Alternate Configurations,** click **Add**.
5. Specify or update values for the listed parameters.
6. Click **Save**. If this is the first alternate configuration you defined, it is saved as Alternate#1. Subsequent configurations are saved as Alternate#2, Alternate#3, and so on.

   To specify the time range for which the configuration you just defined is effective, edit the configuration you just defined using the following procedure, Editing an Alternate Configuration.

Editing an Alternate Configuration

In addition to editing an alternate configuration to change parameter values, you can edit it to specify the time range for which it is effective.

To edit an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click  .
4. From the list of alternate configurations, select the alternate configuration that you want to edit, and then click  .
5. Specify or update values for the listed parameters, including the time range in the From Hour/To Hour.

6 Scroll down to the end of the page and click **Save**.

Editing Alternate Configurations in Bulk

If you need to update the same parameters in multiple alternate configurations, follow the procedure described in "Editing Destination Runtime Parameters" on page 80.

Sending a Command to a Destination

You can send a command to a connector destination.

To send a command to a destination on a connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector for which you wish to send a command. In the management panel, the **Connector** summary tab displays.

3 On the **Connector** summary tab, in the **Destinations** table, click  .

4 Select the command you want to run, and then click **Next**.

5 Enter values for the parameters that the user interface displays, and then click **Finish**.

Deleting a Connector

To delete one or more connectors:

1 Click **Node Management**.

2 In the navigation tree, browse to the container where the connectors reside.

3 In the management panel, click the **Connectors** tab.

4 From the list of connectors, select all connectors the connectors you want to delete.

5 Click **Delete**.

6 Click **OK** to confirm deletion.

7 Reboot the Connector Appliance or Logger system that each connector was associated with.

You can also delete a specific connector from its **Connector** summary tab. Click at the top of the tab to delete the connector.

Sending a Command to a Connector

You can send a command to a connector.

To send a command to a connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector to which you wish to send a command. In the management panel, the **Connector** summary tab displays.

3 On the **Connector** summary tab, click  .

4 From the **Command Type** drop-down list, select the command you want to send to the connector, and then click **Next**.

Running Logfu on a Connector

Run Logfu on a connector to parse ArcSight logs and generate an interactive visual representation of the information contained within the logs.

To send a command to a connector:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector to which you wish to run Logfu. In the management panel, the **Connector** summary tab displays.

3 On the **Connector** summary tab, click  .

4 The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.

- In the **Group** box, choose which type of data you would like to view. The **Group** box lists all connectors within the chosen container, plus many other types of data such as memory usage and transport rates.
- Then, choose one of the Group box data points. Depending on which data point you chose, a list of fields appears in the Field box below.
- Choose a **field** to view. A graphic chart appears in the Chart box, providing rate and time information. The key at the bottom of the Chart box defines the data points mapped in the chart.
- To choose a different data point for analysis, click **Reset Data**.

5 When complete, close the display window.

Changing the Network Interface Address for Events

ArcSight Management Center has multiple network interfaces. By default, the connector determines which network interface address is used for events displayed in the ArcSight Console or Logger, but typically uses `eth0`.

To use a specific network interface address for events, add the parameter `connector.network.interface.name` to the Connector's `agent.properties` file. For example, to use the IP address for `eth1`, specify the following parameter:

```
connector.network.interface.name=eth1
```

Developing FlexConnectors

FlexConnectors are custom SmartConnectors that can read and parse information from third-party devices and map that information to ArcSight's event schema.

ArcSight Management Center provides a FlexConnector Development wizard that lets you quickly and easily develop a FlexConnector by creating a parser file, and enables you to test and package your new FlexConnector before deploying it. The wizard generates regular expressions and provides event field mapping suggestions automatically so you do not need to be an expert in regular expression authoring, parser syntax, or ArcSight event schema.

Use the FlexConnector Development wizard to develop FlexConnectors for simple log files. For complex log files, use the FlexConnector SDK (available from the HP ArcSight Customer Support site)

The FlexConnector Development wizard supports Regex Files, Folder Follower, and Syslog (Daemon, File, Pipe) FlexConnectors only.

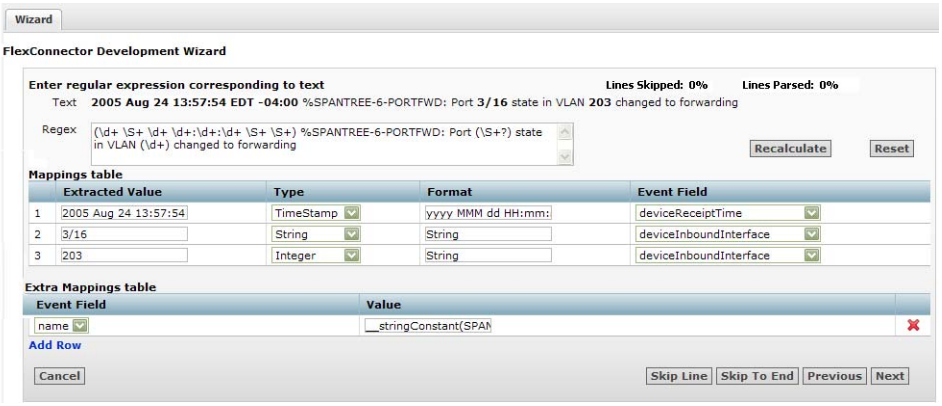
The FlexConnector Development wizard does not support the extra processors property or multiple sub-messages. If you need these features, use the FlexConnector SDK to create your FlexConnector.

A FlexConnector that you develop with the FlexConnector Development wizard might perform more slowly than an HP ArcSight SmartConnector.

To develop a FlexConnector:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where you wish to develop the connector.
3. In the management panel, click the **Connectors** tab.
4. On the **Connectors** tab, click  . The FlexConnector Development wizard is launched.
5. Provide the vendor and product name of the device for which you are creating a FlexConnector, and then click **Next**.
6. Select the data source type, and then click **Next**:
   - Select **Syslog** to create a Syslog FlexConnector to read events from Syslog messages.
   - Select **File** to create a FlexConnector to parse variable-format log files using regular expressions (ArcSight FlexConnector Regex File) or to parse variable-format log files in batch mode (ArcSight FlexConnector Folder Follower).
7. Upload a sample log file for the data source type you selected in the previous step, and then click **Next**.

8 The wizard finds the first unparsed line in the log file, generates a regular expression to match and extract tokens from that line, and displays the suggested field mappings for each extracted token in the Mappings table.



Note

The mappings are displayed in descending order of probability (based on HP ArcSight training data). You can change the mappings by selecting from the list.

The percentage of parsed lines in the file is shown in the top right of the panel. You can use this percentage to estimate where you are in the log file. The percentage of unparsed lines skipped in the file is also shown in the top right of the panel.

- To change the regular expression in the **Regex** box and recalculate the mappings, edit the expression and then click the **Recalculate** button. You can set the regular expression back to the suggested value by clicking the **Reset** button.
- Field mappings that do not correspond directly to the extracted tokens in the unparsed line of the log file are displayed in the Extra Mappings table. You can change the Event Field and provide a token operation. To add a new Event Field, click **Add Row**.

  You can use extra mappings to:

  - Remap an extracted token to a different Event Field in addition to the existing mapping. For example, you can add an Event Field with the value `$3` where `$3` is the third token in the list of suggested mappings.
  - Map a modified token or combination of tokens to an Event Field. For example, you can add an Event Field with the value `__operation($1,$3)`.
  - Map an Event Field to a constant string or integer. For example, you can add an Event Field with the value `__stringConstant(constant)`.

  For a list of the token operations used when tokens are mapped to ArcSight event fields, refer to the FlexConnector Developer's Guide (available from the ArcSight Customer Support site).

9 Click **Next** to save the mapping to the parser file and display the next unparsed line in the log file.

After all unparsed lines in the log file have corresponding regular expressions and mappings, the wizard displays the parser file for review.

10 Review the parser file and make changes, if necessary, directly in the Review Parser File panel.

11 Click **Next** to save and package the parser file.

12 Choose how you want to deploy the FlexConnector:

- Select **Deploy parser to existing connector in container**, and then click **Next** to use the parser file with an existing connector. Click **Done** to close the FlexConnector wizard and re-display the **Container** tab.

The **Deploy parser to existing connector in container** option displays only if the container already contains a connector of the same type.

- Select **Add new connector to container,** and then click **Next** to add the parser as a new connector. Follow the steps to add the connector to the container.

You can share FlexConnectors with other users. See "Sharing Connectors in ArcExchange" on page 86.

Editing FlexConnectors

After you have developed a FlexConnector with the FlexConnector wizard and have deployed it in a container, you can edit the FlexConnector to make changes to the parser file when needed.

The FlexConnector Edit wizard is available on the **Connectors** tab in the **Action** column.

Click  in the **Action** column for the FlexConnector to open the wizard. To edit the parser file, follow Step 5 through Step 12 in "Developing FlexConnectors" on page 83.

Only edit a FlexConnector that is created with the FlexConnector wizard. Editing manually-created FlexConnectors might produce unpredictable results.

Sharing Connectors in ArcExchange

You can share FlexConnectors and parser overrides with other users.

A FlexConnector is a custom connector that you define to gather security events from log files, databases, and other software and devices. You can share the following FlexConnector types:

- Syslog FlexConnectors (to read events from syslog messages)
- Log File FlexConnectors (to read fixed-format log files)
- Regular Expression Log File FlexConnectors (to read variable-format log files)
- Regular Expression Folder Follower FlexConnectors (to read variable-format log files recursively in a folder)
- Regular Expression Multiple Folder Follower FlexConnectors (to read events in real time or batch mode from multiple folders)
- XML FlexConnectors (to read events recursively from XML-based files in a folder)

A parser override is a file provided by HP ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added. You can share parser overrides for all connector types that use a parser.

To share a FlexConnector or parser override, you need to package and upload it to ArcExchange on the HP ArcSight online community (Protect 724) or to your local machine. You can also download a FlexConnector or parser override that you need from ArcExchange or from your local machine and add it to a container.

ArcExchange will not be able to reach the HP ArcSight Protect724 Community if access is attempted through a proxy server.

Packaging and Uploading Connectors

Before uploading your FlexConnector or parser override to Protect 724 or to your local computer, you need to package it into a zip file, (called an AUP package) using the upload wizard.

A FlexConnector AUP package contains the connector properties file, categorization file, connector parameters, and a manifest file with all the metadata on the package required for successful deployment. Metadata includes information about the AUP package, such as the package type, connector type, connector description, and so on. You can create only one AUP package per connector per device type. You can package a FlexConnector in Basic or Advanced mode. In **Basic** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package.
- The wizard packages the categorization file automatically *only* if it can be determined based on the device vendor and product information found in the properties file.
- The wizard does not package connector parameters. You are prompted to configure the connector when it is downloaded and deployed.

In **Advanced** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package. (This is same as Basic mode.)
- The wizard packages the categorization file automatically if it can be determined based on the device vendor and product information found in the properties file. If the categorization file cannot be determined, you are prompted to select the categorization file you want to package from the list of files found in the container.
- The wizard displays connector parameters so you can configure the parameters you want to display and set the default values you want to provide during connector deployment (download). The parameters you do not configure for display are pre-configured with the current values and will not be displayed during connector deployment.

A parser override package contains the parser override properties file and the manifest file only.

Follow the steps below to package and upload a FlexConnector or parser override.

- To upload to ArcExchange, you must have a valid username and password for Protect 724.
- Make sure that you have configured network settings under **Administration** > **System Admin** > **Network** and that ArcSight Management Center can communicate with the Protect 724 server.

To package and upload a FlexConnector or parser override:

1 Click **Node Management**.

2 In the navigation tree, browse to the connector for which you wish to upload a package. In the management panel, the **Connector** summary tab is displayed.

3 On the **Connector** details page, click  .The upload wizard is launched.

4 Click **Next** and follow the steps in the wizard to:

a Select the type of AUP package you want to create for the selected connector.

ArcSight Management Center scans the container and displays the relevant files that can be packaged.

b For a FlexConnector, select **Basic** to create a default package or select **Advanced** to customize the package to meet your needs. For a description of Basic and Advanced mode, refer to "Packaging and Uploading Connectors" on page 87.

c If the connector contains several properties files, you are prompted to select the properties file you want to package. Certain connectors, for example, syslog connectors, can have more than one parser override folder, in this case, you are prompted to select the folder you want to package.

d If you selected Advanced mode for a FlexConnector in Step b and the categorization file cannot be determined, you are prompted to select the categorization file you want to package from a list of files found in the container.

Categorization files are not packaged for parser overrides.

e If you selected Advanced mode for a FlexConnector in Step b, select the configuration parameters you want to display when the connector is deployed and then provide default values for these parameters. Parameters you do not select are pre-configured with the current values.

If any advanced connector parameters were previously modified from their defaults, the wizard displays these parameters so that you can select which ones you want to be configured automatically during deployment.

Configuration parameters are not displayed for parser overrides.

If the connector has table parameters, they are not displayed during packaging. However, when the connector is downloaded to a container, you are prompted to provide values for all the table parameters.

f Provide a description of the AUP package and instructions on how configure the device used by the connector.

g Provide the vendor, product, and version of the device used by the connector.

If the wizard can determine the vendor, product, and version of the device, the information is displayed in the fields provided. You can change the information to meet your needs.

h Upload the created AUP package to ArcExchange or to your local machine. You will require a username and password for Protect 724.

Downloading Connectors

You can download a FlexConnector or parser override that is available from ArcExchange on Protect 724 or from your local computer. You download a FlexConnector or parser override directly to a container.

You can download only one FlexConnector per container using the download wizard. However, there is no limit to the number of parser overrides you can download to a container.

Note

- When downloading a parser override to a container, the download wizard overwrites any existing parser override with the same name in the container without prompting for confirmation. To avoid overwriting an existing parser override, send a **Get Status** command to the existing parser override to check the parser information before you download a new parser override. For information on sending a Get Status command, refer to "Sending a Command to a Connector" on page 82.
- Always back up the container to the Backup Files repository before downloading a connector or parser override so you can revert to the previous configuration if the download produces unexpected results.

Follow the steps below to download a FlexConnector or parser override to a container.

To download to ArcExchange, you must have a valid username and password for Protect 724. Also, make sure that you have configured network settings under **Administration** > **System Admin** > **Network** and that the appliance can communicate with the Protect 724 server.

To download a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the container resides.
3. In the management panel, click the **Containers** tab.
4. From the list of containers, select the container into which you want to download the connector, and then click  in the **Action** column to open the download wizard.
5. Click **Next** and follow the steps in the wizard to:
   a. Select whether you want to download the connector from ArcExchange on Protect 724 or from your local computer.
   b. Select the AUP package you want to download.

      On Protect 724, you can search for a parser override or FlexConnector AUP package using a keyword or a combination of keywords.

Note

You can only download a parser override package to a container that has a connector of the same type as the package.

You can download only one FlexConnector per container using the download wizard. If the container already contains a FlexConnector of the same type as the one you want to download, you can replace the existing FlexConnector with the one you are downloading, but you cannot create a new one.

c For a FlexConnector, provide connector configuration parameters, if needed.

Pre-configured and advanced parameters are deployed automatically with the values that were packaged; you are not prompted to configure these parameters. The configurable parameters are displayed with suggested defaults, which you can modify if necessary. The table parameters are displayed with no configured values, you have to provide the values manually, as needed.

d Add or select a destination for the connector.

If you are downloading the connector to a container that has an existing connector of the same type, you are *not* prompted for a destination.

The wizard copies the properties and categorization files to the appropriate locations and also installs the zip file for the AUP package in the `user/agent/deployedaups` folder on ArcSight Management Center to keep track of the deployment history.

After a successful download, the container is restarted automatically.

Configuration Suggestions for Connector Types

The following table provides configuration suggestions for different types of connectors.

Connector Type	Effects of Limited Usage
Syslog connectors	Due to the nature of UDP (the transport protocol typically used by Syslog), these connectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache might fill and the operating system drop UDP messages. **Note**: Do not use the **Limit CPU Usage** option with these connectors because of the possibility of event loss.
SNMP connectors	Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they can potentially lose events. SNMP is also typically UDP-based and has the same issues as Syslog.
Database connectors	Because connectors follow the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. However, no events will be lost, unless the database tables are truncated. After the event burst is over, the connector might eventually catch up with the database if the event rate does not exceed the configured limit.
File connectors	Similar to database connectors, file-based connectors *follow* files and limiting their event rates causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. The connectors might catch up if the event rate does not exceed the configured rate.
Asset Scanner connectors	All connectors on ArcSight Management Center run as a service (not as an application). Therefore, asset scanner connectors running on are *not* supported in Interactive mode. To run the asset scanner connector in Interactive mode, install the connector on a standalone system and manage it as a software-based connector.

Connector Type	Effects of Limited Usage
Proprietary API connectors	The behavior of these connectors depends on the particular API, (for example, OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. These connectors work much like database or file connectors.

Deploying FlexConnectors

FlexConnectors are custom connectors that are user-defined. FlexConnectors can be hosted on the system if they are compatible with a Linux platform. ArcSight Management Center ships with several prototype FlexConnectors, including:

- ArcSight FlexConnector File
- ArcSight FlexConnector ID-based Database
- ArcSight FlexConnector Multiple Database
- ArcSight FlexConnector Regular Expression File
- ArcSight FlexConnector Regular Expression Folder File
- ArcSight FlexConnector Simple Network Management Protocol (SNMP)
- ArcSight FlexConnector Time-based Database
- ArcSight FlexConnector XML File

You can create and manage FlexConnectors using repositories. You can share FlexConnectors with other users. Refer to "Sharing Connectors in ArcExchange" on page 86.

For more information, consult the FlexConnector Developer's Guide, available from HP ArcSight Customer Support.

Configuring the Check Point OPSEC NG Connector

The Check Point FW-1/VPN-1 OPSEC NG connector can operate in clear channel or sslca mode.

- This procedure is supported only for HP ArcSight connector release 4.6.2 or later.
- A hostname is called an Application Object Name on Check Point. A password is a Communication Activation Key on Check Point.

To configure a connector to operate in sslca mode

On the Check Point SmartDashboard:

1 Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object.

Parameter	Description
Name	A meaningful name for the application object you are creating; for example, ArcSightLea-1. This name is used to pull the OPSEC certificate in the system.

Parameter	Description
Host	The hostname of the HP ArcSight Management Center.
Client Entities	Select LEA.
Secure Internal Communication	If a DN string is not present, initialize the communication by providing an activation key. The activation key is used when the certificate is pulled. This is the SIC Name. Click **Communication** > **Initialize**.

After the object is created, note down the following information, which you will need to provide when continuing configuration.

- *SIC Name:* DN string that you obtain after initializing communication as described below.
- *SIC Entity Name:* Double-click the Check Point Gateway name in the SmartDashboard to view its general properties. The SIC Entity Name is the SIC string configured in the general properties window.
- Check Point IP address or hostname.

2 Pull the Check Point certificate.

To do so, run the `Pull OPSEC Certificate` command on the container to which you will be adding the connector. For detailed information about running a command on a container, see "Sending a Command to a Container" on page 64. You need to provide this information when running the command:

Parameter	Description
Server hostname or IP address	The name or IP address of the Check Point server.
Application object name	The OPSEC Application object name you specified in the previous step. This parameter is case sensitive.
Password	The activation key you entered when creating the OPSEC application object in the previous step.

If the certificate is pulled successfully, a message similar to this is displayed:

```
OPSEC SIC name (CN=ArcSightLea-1,0=cpfw1.5ad8cn) was retrieved
and stored in /opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/<name>. Certificate was
created successfully and written to
"/opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/ArcSightLea-1.opsec.p12".
```

Note down the OPSEC SIC Name (`CN=ArcSightLea-1,0=cpfw1.5ad8cn` in the above example) and the file name (`ArcSightLea-1.opsec.p12` in the above example).

If the certificate is not pulled successfully, check to ensure that the Application object name you specified is correct (including the case) and the container on which you are running the command is up and running.

3 Install Policy on the LEA client for the Check Point Gateway using the SmartDashboard.

On

4 Add a Check Point connector by following instructions described in "Adding a Connector" on page 72. You need to provide the following information.

Parameters	Values to input
Type	Check Point FW-1/VPN-1 OPSEC NG
Connection Type	SSLCA
Connector Table Parameters	Server IP: The IP address of the Check Point server. Server Port: The port on the server that listens for SSLCA connections. Use the default value 18184. OPSEC SIC Name: The name you noted in Step 1. OPSEC SSLCA File: The name you noted after pulling the certificate in Step 2. OPSEC Entity SIC Name: The name you noted in Step 1.

5 An error similar to the following is displayed.

```
-1:[X] Unable to connect to the Lea Server[10.0.101.185] -1:1
connection test failed!
```

Select the **Ignore warnings** check box, and then click **Next**.

6 Continue to configure the rest of the connector. Go to Step 9 in "Adding a Connector" on page 72.

Adding the MS SQL Server JDBC Driver

When you install and configure database connectors that use Microsoft SQL Server as the database, a JDBC driver is required. This driver does not ship pre-installed on the system; you need to install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1 Download the MS SQL Server JDBC Driver to a computer that can access. You can download the driver from Microsoft at:

http://msdn.microsoft.com/en-us/sqlserver/aa937724

2 Run the setup program to install the driver.

3 Follow the instructions in "Uploading Files to a Repository" on page 140 to add the `sqljdbc.jar` file.

The name of the `jar` file may be different from that of some JDBC driver versions. Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database.

The new driver file is added to the repository, as shown in the following example.

After you have installed the JDBC driver, you need to upload the driver file to the containers that will contain the SQL Server database Connectors. Follow the instructions in "Uploading a File from the Repository" on page 142.

After the driver file has been uploaded to a container, follow the instructions in “Adding a Connector” on page 72 to add a connector that requires a JDBC driver.

Adding the MySQL JDBC Driver

When you install and configure database connectors that use MySQL as the database, a JDBC driver is required. This driver does not ship pre-installed on the system. Install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1. Download the MySQL JDBC Driver to a computer that can access ArcSight Management Center. You can download the driver from:

   http://dev.mysql.com/downloads/connector/j/5.0.html

2. Extract the driver.

3. Follow the instructions in “Uploading Files to a Repository” on page 140 to add the `mysql-connector-java-x.x.x-bin.jar` file.

   The new driver file is added to the repository.

   After you have installed the JDBC driver, you need to upload the driver file to the containers that will contain the MySQL database Connectors. Follow the instructions in “Uploading a File from the Repository” on page 142.

   After the driver file has been uploaded to a container, follow the instructions in “Adding a Connector” on page 72 to add a connector that requires a JDBC driver.

Chapter 7

Managing Configurations

The following topics are discussed here.

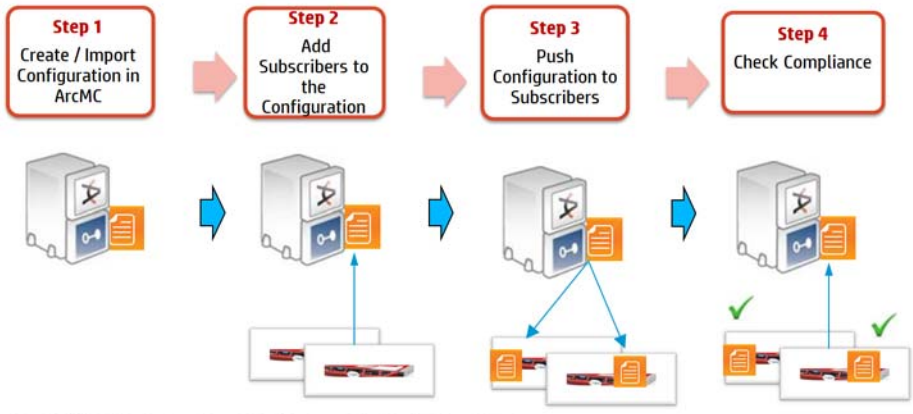
Overview

A *configuration* is a group of settings and their associated values, which can be pushed to nodes managed by ArcSight Management Center. You can to assign easily values to, propagate, and maintain the same settings across multiple nodes of the same type. Using configurations speeds and eases management of multiple managed ArcSight products.

Nodes can be *subscribed* to a particular configuration, so they can receive a new, updated, or edited configuration from ArcSight Management Center.

You can also check whether the settings and their values on a node match the ones for a configuration type; if so, the node is said to be in *compliance* with the configuration.

Illustrated here is a possible workflow.



For example, you can set up a suitable DNS configuration for an appliance (see Table 7-4 on page 113), specifying primary DNS server, secondary DNS server, and search domains for the appliance. You can then push that configuration to subscribing appliances, and so ensure that the DNS settings for all subscribers are configured identically with a single action.

If you later updated the configuration to use a new primary DNS server, you could push the new configuration to all subscribers, and all of them would be updated for the new DNS server with one action.

You could, at any time, verify each node's compliance with the configuration to determine if its settings were assigned the desired values.

Each configuration is defined by a set of parameters specific to the type of node to which it applies. These parameters are listed under "Configuration Types" on page 107.

You can perform the following configuration management tasks:

- Create, edit, and delete a configuration
- Import a configuration from a node to ArcSight Management Center, for use on other nodes
- Add or remove subscribers to a configuration
- Push a configuration to subscriber nodes
- Check the compliance of subscriber nodes with a selected configuration

Configuration Types

A configuration is assigned a *type*. A configuration may only be pushed to a node that is appropriate for its type.

You can create any number of configurations of the same type. For example, you could specify several different SMTP configurations, specifying different mail servers in each one. However, each node may only subscribe to a single configuration of each type.

Configuration types include the following:

- Connector Configurations:
  - FIPS
  - Map File
  - Parser Override
  - Syslog Connectors
- Connector Appliance Configuration:
  - Connector Appliance Configuration Backup:
- Logger Configurations:
  - Logger Configuration Backup
  - Logger Filter
  - Logger SmartMessage Receiver
  - Logger Storage Group
  - Logger Transport Receiver

- System Admin Configurations:
  - Authentication External
  - Authentication Local Password
  - Authentication Session
  - DNS
  - Network
  - NTP
  - SMTP
  - SNMP
  - Users

For details on the settings associated with each configuration type, see "Configuration Types" on page 107.

Configuration Management

To create or manage configurations, on the menu bar, click **Configuration Management.**

To access a specific configuration type, select the configuration type from the sub-menu. For example, to access all configurations for Loggers, click **Configuration Management > Logger Configurations.**

The Configurations Table

The **Configurations** table lists all currently available configurations in ArcSight Management Center. Each listed configuration, whether it was created in ArcSight Management Center or imported from an existing node, is considered the definitive (or "golden") copy of that configuration, for pushing to managed nodes. The table includes the following columns:

- **Name:** The name of the configuration
- **Type:** The type of configuration.
- **Last Edited By:** The most recent user to edit the configuration.
- **Compliant:** Compliant status is an aggregation of the status of the individual subscribers to that configuration.
  - *Yes* indicates that all subscribers are in compliance.
  - *No* indicates that at least one subscriber is out of compliance.

- *Unknown* indicates that the compliance status for one or more subscribers cannot be determined (for example, because connectivity to a subscriber is not available).

You can check the individual compliance of each subscriber on the **Subscribers** tab.

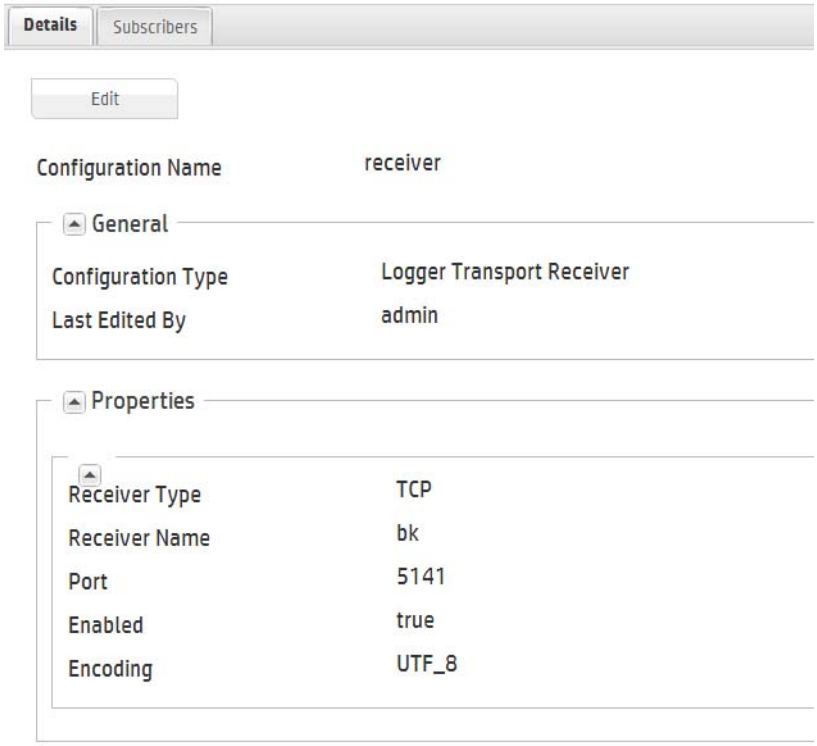
Click any column header to sort the **Configurations** table by that column.

To view the details of any configuration, select it in the list. The **Details** and **Subscribers** tabs at the bottom of the page will display additional information.

To select multiple items from any list, Shift+Click or Ctrl+Click while selecting.

The Details Tab

The **Details** tab shows the specifics of the configuration, including any configured attributes and their values.



General

General details describe the basics of the configuration, as follows:

- **Configuration Name:** The name of the configuration. Each configuration name must be unique, and may be up to 255 characters in length.

- **Configuration Type:** The type of the configuration. Types of configuration include Logger, System Admin, Software Connector, and Connector Appliance. For details of configuration types, see "Configuration Types" on page 107.
- **Last Edited By:** The most recent user to edit the configuration.

Properties

A *property* is a group of one or more settings for the configuration. For example, for the NTP Server configuration, the property includes two settings: Enable as NTP Server, and NTP Servers (a list of NTP servers).

The exact parameters included in each property are pre-defined for each configuration type. ArcSight Management Center prompts for values of each setting when the property is selected. Each parameter must be assigned a valid value corresponding to its data type. For instance, if the data type is integer, you must enter an integer value. A red asterisk (*) indicates a required parameter.

As an example, to create a SNMP configuration, described in Table 7-4 on page 113, you would need to supply values for Enable SNMP Polling (a Boolean value), Community String (a string value), and Port Number (an integer).

List Configurations

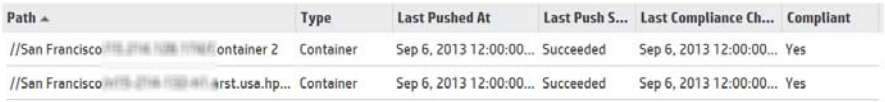
A donfiguration type that can include more than one property is known as a *list configuration*. A list configuration represents a configuration with multiple data values of the same kind. For example, the Users Configuration could include information on multiple users; each Property would represent a different user (with different first and last names, contact details, and other personal data).

A pushed list configuration will override any existing configuration of the same type on the managed node.

For a description of supported configuration types, the parameters associated with each type, and their data types, see "Configuration Types" on page 107.

The Subscribers Tab

The **Subscribers** tab lists all managed nodes currently eligible to receive the configuration. (The list is empty if no hosts have been added yet.) The list includes the following columns:



Path	Type	Last Pushed At	Last Push S...	Last Compliance Ch...	Compliant
//San Francisco ontainer 2	Container	Sep 6, 2013 12:00:00...	Succeeded	Sep 6, 2013 12:00:00...	Yes
//San Francisco arst.usa.hp...	Container	Sep 6, 2013 12:00:00...	Succeeded	Sep 6, 2013 12:00:00...	Yes

- **Path:** The path of the subscribing node, consisting of location/hostname/node type.
- **Type:** The type of subscribing node.
- **Last Pushed At:** The time and date of the most recent push to the subscriber.
- **Last Push Status:** The status of the most recent push to the subscriber.
  - *Succeeded*: the configuration push was successful.
  - *Failed*: hover over the link to determine the reason for the push failure. An error message is displayed to help in remediation of the issue. For more information, see "Push Remediation" on page 105.

- *Unknown:* Initial status before the subscriber has received any pushes.

- **Last Compliance Check:** The date and time of the most recent compliance check.
- **Compliant:** indicates whether the node is in compliance with the configuration.
  - *Yes* indicates the node is in compliance. (The values for *all* settings associated with the configuration type match the values from the configuration.)
  - *No* indicates the node is out of compliance. (One or more values for the settings associated with the configuration type do not match the values from the configuration.) Hover over *No* to show the cause of the node's non-compliance.
  - *Unknown* indicates that the node's compliance could not be determined at the time of the most recent compliance check, or that the node has not yet undergone a compliance check.

Non-Compliance Reports

For a compliance status of *No* or *Unknown*, hover over the field to display a tooltip showing report on the node's non-compliance. The tooltip is in the following format:

```
setting_name1:<configuration value>:<node
value>|setting_name2:<configuration value>:<node value>|...
```

where `setting_nameN` is each differing setting in the configuration, `<configuration value>` is the setting's value in the configuration in ArcSight Management Center, and `<node value>` is the setting's value on the non-compliant node. Each problematic setting and its values are separated by a pipe character (|).

If the property type is a list, then the list value will be enclosed in a pair of square brackets; for example, `[item1, item2]`.

Creating a Configuration

You can create a configuration for pushing to any subscribed nodes.

The following configuration types may only be imported from managed nodes, not created in ArcSight Management Center:

- Logger Storage Group
- Logger Filter
- Authentication External
- Users

For more information on importing a configuration from a managed node, see "Importing a Configuration" on page 102.

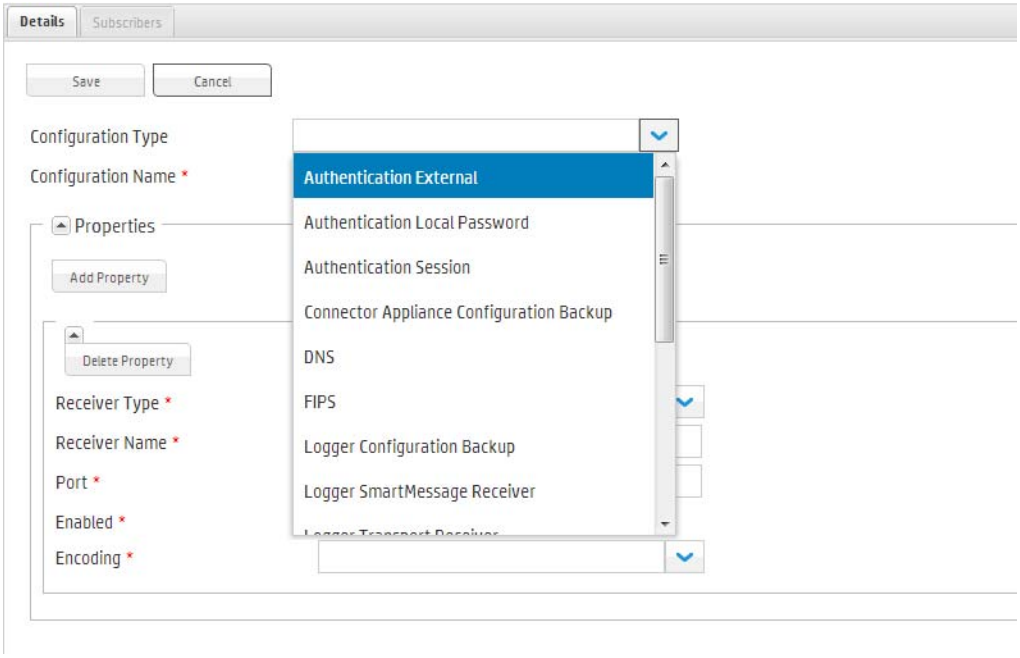
To create a configuration:

1. Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2. Under **Configurations**, click **New**.
3. On the **Details** tab, select a configuration type from the **Configuration Type** drop-down list. (Only the configuration types appropriate for the node type are shown in the drop-down list.)

4 In **Configuration Name,** enter a name for the configuration. (Configuration names must be unique and may be up to 255 characters in length.).



5 Enter valid values for each of the required parameters, indicated with a red asterisk *.

Note

For a description of valid parameters for each configuration type, and the data type associated with each, see "Configuration Types" on page 107.

6 Optionally, to add an additional property for a list configuration: click **Add Property**, and then enter values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.

7 Click **Save**.

Editing a Configuration

You can adjust or delete values for a configuration. You may not edit a configuration currently being pushed.

To edit a configuration:

1 Click **Configuration Management.**

Tip

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 From the **Configurations** table, select the configuration to be edited.

3 On the **Details** tab, click **Edit**.

- Edit the general settings as needed.

- Optionally, to add an additional property for a list property: click **Add Property**, and then enter values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
- Optionally, to delete a property from the configuration, click **Delete Property.**

4 When complete, click **Save**. After saving, if the configuration has any subscribers, you are prompted to push the updated configuration to the subscribers.

Deleting a Configuration

A deleted configuration is no longer available for pushes to subscribers. You may not delete a configuration currently being pushed.

To delete a configuration:

1 Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 From the **Configurations** table, select one or more configurations to be deleted.

3 Click **Delete.**

4 Click **OK** to confirm deletion.

Importing a Configuration

A configuration created on a managed node may be imported into ArcSight Management Center, for editing and pushing to other nodes of the same type.

For example, you can define a configuration on a managed Connector Appliance, and then import the configuration into ArcSight Management Center. The imported configuration may then be edited and pushed to other managed Connector Appliances, just the same as you would with a configuration you originally created in ArcSight Management Center.

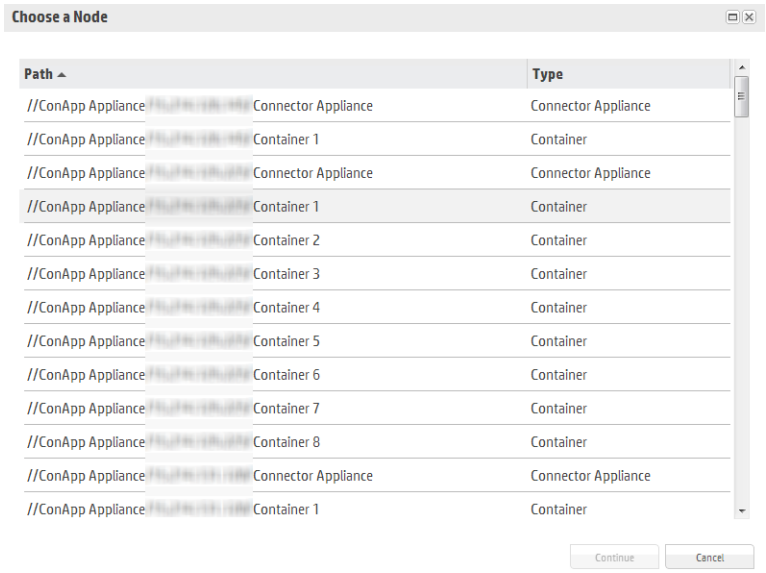
To import a configuration:

1 Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 Under **Configurations**, click **Import**.

3 On the **Choose a Node** dialog, select the node from which you wish to import the configuration.



4 Click **Continue**.

5 On the **Import Configuration** dialog:

a Select a configuration type for the imported configuration from the **Type** drop-down list. (The entries in the list depend on the configuration types which apply to the node chosen in Step 3.)

a In **Name**, enter a name for the imported configuration.

6 Click **Import**. The configuration is imported into ArcSight Management Center and is shown in the **Configurations** table.

Managing Subscribers

A *subscriber* is a managed node to which a configuration may be pushed. Each node can subscribe to *only one* configuration of each configuration type.

For example, a Logger appliance could subscribe to one Logger Storage Group configuration, but the same appliance could also subscribe to a Logger Filter configuration as well as a Logger Transport Receiver configuration.

Adding a Subscriber

A subscribed node can receive a pushed configuration.

To subscribe a node to a configuration:

1 Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 From the **Configurations** table, select a configuration.

3 Click the **Subscribers** tab.

4 Click **Add Subscribers.**

5 On the **Add Subscribers** dialog, select a node to add as a subscriber. The list of potential subscribers is determined by the selected configuration type. To select multiple nodes for subscription, Ctrl+Click each node.

A node may only subscribe to one configuration of each type; for example, one DNS configuration.

If you attempt to add a subscriber which is already subscribed to a configuration of the same type, the following message is displayed: *No available subscribers have been found for the selected configuration.*

6 Click **Add Subscribers.**

7 Click **OK** to confirm completion. The subscriber is added to the configuration.

Unsubscribing a Subscriber

After being unsubscribed, a subscriber can no longer receive a pushed configuration.

To remove a subscriber from a configuration:

1 Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 From the **Configurations** table, select a configuration.

3 Click the **Subscribers** tab.

4 Select one or more subscriber from the list of subscribers.

5 Click **Unsubscribe**.

6 Click **OK** to confirm. The selected subscribers are removed from the list.

Pushing a Configuration

The push process synchronizes a configuration from ArcSight Management Center to *all* of the configuration's subscribers. Pushing must be performed manually.

To push a configuration to all subscribers:

1 Click **Configuration Management.**

To select a specific configuration type, select the desired configuration type from the **Configuration Management** menu: **Logger Configurations, System Admin Configurations, Connector Configurations,** or **Connector Appliance Configurations**.

2 From the **Configurations** table, select a configuration to be pushed.

3 Click **Push**.

4 Click **OK** to confirm the push. The configuration is pushed to all subscribers of the selected configuration.

Push Validation

During a push to subscribers, the configuration is automatically validated by ArcSight Management Center. Validation ensures that a pushed configuration contains appropriate, meaningful values for all settings. If any values are invalid, the push will fail, and an error message is returned. Hover over the subscriber's entry on the Subscribers tab, in the **Push Status** column, to show the cause of the failed push.

For example, as shown in , the Size value of a Logger Storage Group must be an integer. However, a Logger Storage Group configuration with a negative integer value for Size would be an invalid configuration, and the push of such a configuration would fail.

Common Causes for Push Failure

A push to a subscriber may fail for any number of reasons. These may include:

- **Validation Failure:** A push with invalid content will fail. Verify that your configuration includes valid setting values for the configuration type.
- **Lack of Connectivity:** Network or system issues can cause disrupt connectivity to a subscriber. Verify connectivity with the subscriber.
- **Agent Not Running on Connector Appliance or Logger:** In order to receive a push on Connector Appliance or Logger (both hardware and software form factors), the ArcSight Management Center Agent must be running on the subscriber. Verify that the Agent process is active on the subscribing node.
- **Privileges on Subscribing Host:** In order to push a subscription, the **ArcSight Management Center** user (specified by the user credentials) must have privileges to view, edit, or delete configuration settings on the subscriber nodes.
- **Licensing:** An expired host license will cause the push to fail.

Push Remediation

If a push to a subscriber fails, select the configuration from the **Configurations** table. Then click the **Subscribers** tab and choose the subscriber. The **Last Push Status** will show *Failed*. Hover over this link to view the error message associated with the push failure.

After viewing the error message, you can take the appropriate steps on the managed node to address the issue. Resolution may require direct or remote access to the node outside of ArcSight Management Center. After the issue is resolved, you can retry the failed configuration push.

Checking Compliance

A node is in *compliance* with a configuration if the configuration listed in the **Configurations** table is installed on the node, and its values match those assigned to the configuration in ArcSight Management Center. A configuration listed in ArcSight Management Center is considered the definitive (or “golden”) copy of the configuration.

For example, you create an SMTP configuration in ArcSight Management Center named *Sample SMTP Configuration,* with these values assigned:

- Primary SMTP Server: *Mailserver1*
- Secondary SMTP Server: *Mailserver2*
- Outgoing Email Address: *admin@example.com*

A node would be in compliance with this configuration if the values for its primary and secondary SMTP servers, and outgoing email address, matched the values in *Sample SMTP Configuration*.

If any one of these values were different (for example, if a node had a primary SMTP Server of *CorporateMail1*) the node would be out of compliance.

You can manually check the compliance of all subscribers to a configuration.

To check subscriber compliance for a configuration:

1 Click **Configuration Management.**

To select a specific node type, select the desired node type from the **Configuration Management** menu: **Loggers, System Admin, Connectors,** or **Connector Appliances**.

2 In the **Configurations** table, select the configuration to be checked for compliance.

3 Click **Check Compliance**. All subscribers to the selected configuration are checked for compliance.

- On the **Configurations** table, the **Compliant** column shows the aggregated compliance of all subscribers.
- On the **Subscribers** tab for the configuration:
  - The **Last Compliance Check** column is updated to show the most recent check.
  - The **Compliant** column indicates the individual compliance of each node.

Configuration Types

The following section lists the available configuration types, the parameters associated with each, their data types, and a brief description of what the parameter represents. When assigning values to parameters:

- Each parameter's value must be of the data type indicated (for example, the String data type indicates that you must enter a string for the value).
- *Required* parameters, marked with a red asterisk (*), must be assigned a value. A configuration missing any required parameter cannot be saved or pushed.
- *Read-only* parameters cannot be edited in ArcSight Management Center.
- For security reasons, password parameters are displayed obfuscated.

For details of each entry field in the UI, in edit mode, hover over the field label to view the descriptive tooltip.

Connector Configuration Types

Connector configurations set values for settings on containers or software connectors. The available software connector configuration types are listed here.

Table 7-1 Connector Configuration Types

Parameter	Data Type	Description
Configuration Type: *FIPS* Enables or disables FIPS mode on a container.		
Enabled*	Boolean	If **Yes**, FIPS is enabled on the container.
Configuration Type: *Map File* Defines the path and content of container map files. • Contains a list of map files and overwrites the map files under "map" directory on the target machine when it is pushed. • Will first delete all the *.properties files under map and then add the list of map files to the target. • If the configuration contains an empty list, it will clear up all the properties file under "map" • List configuration. Each path/content pair represents a single map file. To include multiple files, add multiple Properties to the configuration.		
Path*	String	Path to the map file.
Content*	String	Content of the map file.
Configuration Type: *Parser Override* Defines the path and content of one or more container parser override files. • Contains a list of parser overrides files and overwrites the parser overrides files under the "fcp" directory on the target machine when it is pushed. • Will first delete all the *.properties files recursively under "fcp" directory and then add the list of parser override files to the target. • If the configuration contains an empty list, it will clear up all the properties file recursively under "fcp" directory. • List configuration. Each path/content pair represents a single parser file. To include multiple files, add multiple Properties to the configuration.		
Path*	String	Path to the parser override file.
Content*	String	Content of the parser file.
Configuration Type: *Syslog Connector* Defines values for syslog connector port and protocol. Only pushed to target if a syslog connector exists. *Note: Only connectors of the syslog type are supported in ArcSight Management Center 1.0.*		
Port*	Integer	Syslog connector port.
Protocol*	Enum	Protocol of the syslog connector (either UDP or Raw TCP).

Connector Appliance Configuration Type

Connector Appliance configurations set values for settings on both hardware and software Connector Appliances. The available Connector Appliance configuration type is listed here.

Table 7-2 Connector Appliance Configuration Type

Parameters	Data Type	Description
Configuration Type: *Connector Appliance Configuration Backup* Sets values for scheduled configuration backups of hardware and software Connector Appliance. Backup content includes all backup data. After a push, the web process is automatically restarted on the subscriber. **Note:** You can neither create nor import settings related to a one-time configuration backup.		
IP/Host*	String	IP or hostname of the remote system where the backup will be saved.
Port*	Integer	Port of the remote system. Default value is 22.
Base Remote Directory*	String	Destination directory on the remote system. Must be manually created on remote system prior to push. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
User*	String	User name on destination.
Password*	String	Password on the destination. (Obfuscated.)
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are *Su, M, T, W, Th, F, Sa*.
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00 midnight. For example, a value of 14 would correspond to 2 PM.

Logger Configuration Types

Logger configurations set values for settings on hardware and software Loggers. The available Logger configuration types are listed here.

Table 7-3 Logger Configuration Types

Parameter	Data Type	Description
Configuration Type: *Logger Configuration Backup* Sets values for scheduled configuration backups of hardware and software Logger to a remote system. **Note:** You can neither create nor import settings related to a one-time configuration backup.		
SCP Port*	String	Port of the remote system. Default value is 22.
IP Address/Hostname*	String	IP or hostname of the remote system where the backup will be saved.
Username*	String	User name on destination.
Password*	String	Password on destination. (Obfuscated.)
Base Remote Directory*	String	Destination directory on the remote system. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are *Su, M, T, W, Th, F, Sa*.
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00. For example, a value of 14 would correspond to 2 PM.
Backup Content*	String	Type of content to be included in the backup. Valid values are: • *All:* includes all backup data. • *Report_Content_Only*: includes only report data.
Configuration Type: *Logger Filter* List configuration. Sets values for a saved search on Loggers. Each filter in the configuration is represented by a different Property. **Note:** Filter configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See "Importing a Configuration" on page 102 for more information.		
Filter Name*	String (Read-only)	Name of the filter.
Filter Type*	String	Valid values are *Regex* or *Unified*.

Table 7-3 Logger Configuration Types

Parameter	Data Type	Description
Query*	String	Query string.
Configuration Type: *Logger SmartMessage Receiver* List configuration. Used to manage settings for SmartMessage Receivers. When you push a SmartMessage Receiver type configuration to a Logger, it overwrites any existing SmartMessage receivers; any other type of receivers such as UDP, TCP, and so on are not affected.		
Receiver Name*	String	Name of the receiver.
Enabled*	Boolean	If **Yes**, SmartMessage reception is enabled.
Encoding*	String	Encoding type. Valid values are: • UTF-8 • US-ASCII
Configuration Type: *Logger Storage Group* List configuration. Sets values for a storage group on a Logger. Each storage group in the configuration is represented by a different Property. **Note:** Storage Group configurations can only be imported from managed Loggers, not created in ArcSight Management Center. See "Importing a Configuration" on page 102 for more information.		
Storage Group Name*	String (Read-only)	Name of the storage group. • The pushed configuration must contain the same number of storage groups as configured on the Logger. • The names of the storage groups in the pushed configuration must match the names of storage groups on the Logger.
Maximum Age (Days)*	Integer	Maximum age of events in storage, in days.
Maximum Size (GB)*	Integer	Maximum size of the storage group, in gigabytes. • The cumulative size of all storage groups must not be greater than the storage volume size on the Logger.
Configuration Type: *Logger Transport Receiver* List configuration. Used to manage configurations of UDP, TCP, CEF UDP, or CEF TCP receivers on Logger. (*Note: In Logger documentation, a Transport Receiver is referred to as just a Receiver.*) When you push a Transport Receiver type configuration to a Logger, it overwrites any existing UDP, TCP, CEF UDP, and CEF TCP receivers; any other type of receivers such as SmartMessage are not affected. Each receiver in the configuration is represented by a different Property.		
Receiver Name*	String	Name of the receiver.

Table 7-3 Logger Configuration Types

Parameter	Data Type	Description
Receiver Type*	String	Receiver type. Valid values are: • UDP • TCP • CEF UDP • CEF TCP
Receiver Name*	String	Name of the receiver.
Port*	Integer	Port number. Must be a non-zero positive number.
Enabled*	Boolean	If **Yes**, transport reception is enabled.
Encoding*	String	Encoding type. Valid values are: • UTF-8 • Shift_JIS • EUC-JP • EUC-KR • US-ASCII • GB2312 • UTF-16BE • Big5 • GB18030 • ISO-8859-1 • Windows-1252 For CEF UDP and CEF TCP receivers, only UTF-8 and US-ASCII apply. **Caution:** Selection of the wrong encoding for a CEF receiver will cause a push failure.

System Admin Configuration Types

System Admin configurations set values for system administrative settings. The available System Admin configuration types are listed here.

Table 7-4 System Admin Configuration Types

Parameter	Data Type	Description
Configuration Type: *Authentication External*		
Defines values and behavior for a system requiring authentication to an external server, such as LDAP or RADIUS. Applies to hardware and software form factors. After changing the Authentication Method on a host, you must delete the host from ArcSight Management Center, and then re-add it using Node Management. **Note:** Authentication External configurations can only be imported from managed nodes, not created in ArcSight Management Center. See "Importing a Configuration" on page 102 for more information.		
Authentication Method*	String	System authentication method.
Allow Local Password Fallback for Default Admin Only*	Boolean	If **Yes**, the authentication server will fall back to local passwords for authentication for administrators.
Allow Local Password Fallback for All Users*	Boolean	If **Yes**, the authentication server will fall back to local passwords for authentication for all users.
LDAP Server Hostname[port]*	String	LDAP server hostname and port.
LDAP Backup Server Hostname [port]	String	LDAP backup server hostname and port.
LDAP Server Request Timeout (seconds)	Integer	LDAP server request timeout, in seconds.
RADIUS Server Hostname[port]	String	RADIUS server hostname and port.
RADIUS Backup Server Hostname[port]	String	RADIUS backup server hostname and port
RADIUS Shared Authentication Secret	String	RADIUS authentication shared secret.
RADIUS Server NAS IP Address	String	RADIUS server Network Access Server IP address.
RADIUS Request Timeout (seconds)	Integer	RADIUS server request timeout, in seconds.
RADIUS Retry Request	Integer	Number of times to retry RADIUS server requests.
RADIUS Protocol	String	Type of RADIUS protocol.
Configuration Type: *Authentication Local Password*		
Defines the system's local password options and behavior. Applies to hardware and software form factors.		

Table 7-4 System Admin Configuration Types

Parameter	Data Type	Description
Enable Account Lockout*	Boolean	If **Yes**, account lockouts are enabled after an incorrect password entry.
Lock Out Account after N Failed Attempts*	Integer	Number of failed attempts before lockout.
Remember Failed Attempts For (seconds)*	Integer	Time, in seconds, between failed attempts that will trigger a lockout.
Lockout Account for (minutes)*	Integer	Time, in minutes, that the account will be locked out.
Enable Password Expiration*	Boolean	If **Yes**, password expiration is enabled
Password Expires in (days)*	Integer	Interval, in days, after which a password expires.
Notify User (Days Before Expiration)*	Integer	Days before password expiration that the user is notified.
Users Exempted from Password Expiration Policy	List of comma-separated strings	Comma-separated list of users whose passwords will never expire.
Enforce Password Strength*	Boolean	If **Yes**, password strength is enforced.
Minimum Length (characters)*	Integer	Minimum number of password characters.
Maximum Length (characters)*	Integer	Maximum number of password characters.
Numeric [0-9]*	Integer	Minimum number of numeric password characters.
Upper Case [A-Z]*	Integer	Minimum number of uppercase password characters.
Lower Case [a-z]*	Integer	Minimum number of lowercase password characters
Special [1$^*...]*	Integer	Minimum number of special password characters.
Password Must Be At Least*	Integer	Minimum number of characters a new password must differ from the user's previous password.
Include "Forgot Password" link on Login Screen*	Boolean	If **Yes**, a link is provided where the user can recover a password.
Configuration Type: *Authentication Session*		
Defines values for the system's authentication sessions. Applies to hardware and software form factors.		

Table 7-4 System Admin Configuration Types

Parameter	Data Type	Description
Max Simultaneous Logins Per User*	Integer	Maximum number of simultaneous logins per user.
Logout Inactive Session After (seconds)*	Integer	Inactivity session timeout, in seconds.
Disable Inactive Account After (days)*	Integer	Number of days of inactivity after which an account will be disabled.
Configuration Type: *DNS* Defines values for the system's Domain Name Service. Applies to hardware form factor only.		
Primary DNS*	String	Primary DNS server.
Secondary DNS	String	Secondary DNS server.
DNS Search Domains	List of comma-separated strings	Comma-separated list of DNS search domains.
Configuration Type: *Network* Defines values the system's default gateway setting. Applies to hardware form factor only. **Note:** Values for these network settings *cannot* be changed through ArcSight Management Center: hostname, IP addresses for the network interfaces, static routes, /etc/hosts file, and time settings.		
Default Gateway*	String	Default network gateway.
Configuration Type: *NTP* Defines values for the system's Network Time Protocol. Applies to hardware form factor only.		
Enable as NTP Server*	Boolean	If **Yes**, the system is enabled as an NTP server.
NTP Servers*	List of comma-separated strings	Comma-separated list of NTP servers. Required even if **Enable as NTP Server** is false.
Configuration Type: *SMTP* Defines values for the system's Simple Mail Transfer Protocol. Applies to hardware and software form factors.		
Primary SMTP Server*	String	Primary SMTP server.
Secondary SMTP Server	String	Secondary SMTP server.
Outgoing Email Address*	String	Outgoing email address.
Configuration Type: *SNMP* Defines values for the system's Simple Network Management Protocol. Applies to hardware form factor only.		
Enable SNMP Polling*	Boolean	If **Yes**, SNMP polling is enabled.
Community String*	String	SNMP community string.
Port*	Integer	SNMP port.

Table 7-4 System Admin Configuration Types

Parameter	Data Type	Description
Configuration Type: Users List configuration. Defines values for system users. Applies to hardware and software form factors. To add multiple users to a node, add multiple properties to the configuration. Pushing a Users Configuration to a node will replace all existing users on the node with the users in the pushed configuration. A Users configuration must include values for the default administrative user, which must be part of the default administrative group. **Note:** Users configurations can only be imported from managed nodes, not created in ArcSight Management Center. See "Importing a Configuration" on page 102 for more information.		
Login*	String	User's login.
Password*	String	User's password. (Obfuscated.)
Active	Boolean (Read-only)	If **Yes**, user is active.
First Name*	String	User's first name.
Last Name*	String	User's last name.
Distinguished Name (DN)	String	If the system uses external authentication, such as LDAP, the user's Distinguished Name in the authentication context.
Email*	String	User's email address.
Phone	String	User's phone number.
Title	String	User's title.
Department	String	User's department.
Fax	String	User's fax number.
Alternate Number	String	User's alternate contact number.
Notes	String	Comments on the user's account.
Groups*	List of comma-separated strings	User's group memberships. Case-sensitive; needs to match group information defined on the subscribing node (such as on Connector Appliance).

Chapter 8

Managing Backups and Restores

The following topics are discussed here:

Overview

The **Backup** and **Restore** menu items enables you to back up and restore your ArcSight Management Center configuration. A complete backup includes all data on managed nodes, configurations, system administration, connector data (in `agentdata` folders), as well as all repository files. Depending on the size and manageability of the backup file, you can include some or all of this data.

Backup

You can back up the current ArcSight Management Center configuration as often as needed, either to a remote system on the network, or to your local system.

To back up the ArcSight Management Center configuration:

1. Click **Administration** > **Backup**.
2. Under **Enter Backup Parameters**, supply values for the parameters listed in the following table:

Parameter	Description
Protocol	Select **SCP** to use Secure Copy to save the backup file on a remote system on your network. You need to specify the IP address or host, your user name and password, and the destination directory in the appropriate fields. Select **Save to Local** to save the backup file on your local system. When you select this option, the **Port**, **IP/Host**, **User**, **Password**, and **Remote Directory** fields are disabled (grayed out) as they are not needed.
Port	SCP only. The default port is 22.
IP/Host	SCP only. The destination to receive the backup file.
User	SCP only. A user name on the destination.

Parameter	Description
Password	SCP only. The password for the user name you specify.
Remote Directory	SCP only. The subdirectory on the specified destination to receive the configuration backup file.
Schedule / One time only	**One Time Only** SCP only. Allows for a “one time only” backup. **Schedule** Provides the option to specify backup times in days, hours, or minutes. Note the following rules for this option: • Valid days of the week are *M, Tu, W, Th, Fr, Sa, Su.* • Letters are not case-sensitive. • Minutes must exceed 15 minute intervals. • **Minute** intervals start at the **top of the hour**, not at the time the request was made. • **Hour** intervals start at **midnight**, not at the time the request was made.
Backup	• Select **All** to create a backup file that contains all data on managed nodes, configurations, system administration, connectors, and repositories. **Tip**: Choosing **All** can potentially create a .tar.gz file so large that the restoration of data is unsuccessful. To prevent this, you may want to exclude connector data and repository data from your backup file. • Select **Exclude Connector Data** to that does not include connector data. • Select **Exclude Repository Data** to create a backup file that does not include files in the repositories. • Select **Exclude Connector and Repository Data** to exclude both connector data and repository files from the backup. **Note**: Restoration of a backup file that includes **connector data** may result in duplicate events generated from the agentdata folders from the time of backup. If you plan to store this backup for a later time, you should exclude connector data.

3 Click **Save** to back up the configuration, and then select a location to save the file.

Restore

You can restore your ArcSight Management Center configuration from a previous backup.

To restore the configuration:

1 Click **Administration** > **Restore**.

2 Under **Upload Backup for Restore**, click **Choose File**.

3 Select your backup file.

4 Click **Upload** to restore the configuration from the specified backup file.

The version of ArcSight Management Center used to restore the backup must be the same version used to create it.

5 Restart the ArcSight Management Center web process.

6 Re-import the SSL certificate for each container. Click the icon to run the **Certificate Download** wizard and import the valid certificates.

After restoring the configuration:

- The cache size on the restore might be different from the cache size in the backup file. For example, after restoring the configuration, connectors might receive more events or consume more cache.
- The container versions on the restore (if any) might be different from those in the backup file.
- The **Cache** column on the **Connectors** tab may take a few minutes to refresh the updated cache size for the connectors.

Chapter 9

Creating Snapshots

The following topics are discussed here.

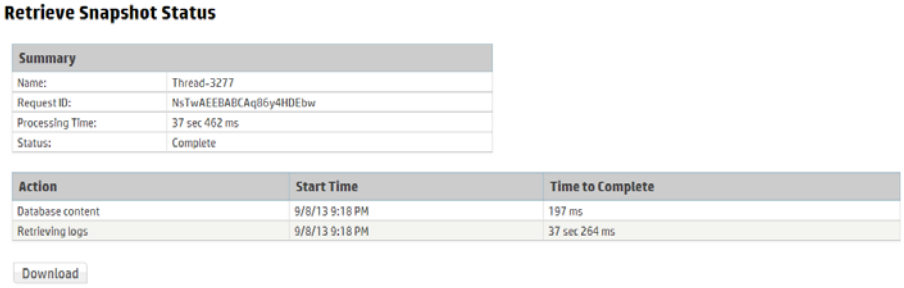
Overview

ArcSight Management Center records audit and debug information, including details of any issues that can occur during normal operations. These system logs form a *snapshot* of your ArcSight Management Center activity. System logs are helpful in troubleshooting issues.

HP ArcSight Customer Support may ask you to retrieve and submit system logs as part of an incident investigation.

Creating a Snapshot

Creating a snapshot of ArcSight Management Center creates a set of logs in a ZIP file, which you can download locally.



To create a snapshot:

1. Click **Administration > Snapshot.**
2. The **Retrieve Snapshot Status** page displays. Depending on the size of the log files, the snapshot may take a few moments to generate.
3. When ready, click **Download** to download the ZIP file locally to a location of your choosing.

Submit the snapshot file as instructed by HP ArcSight Customer Support.

An ArcSight Management Center snapshot does not include information on the activity of the ArcSight Management Center Agent on remotely-managed hosts.

To obtain logs for ArcSight Management Center Agent activity on a managed host, access the remote host. Under **Setup > Appliance Snapshot,** click the **Download** button.

Chapter 10

Managing Repositories

The following topics are discussed here.

Overview

Certain management operations require a specific upgrade or content update (`.enc`) file, or a certificate. Other operations, such as viewing logs, require you to load the logs to a Log repository. ArcSight Management Center can also maintain centralized repositories for files needed for host configuration and management. By default, a number of pre-defined repositories are provided. However, you can create more repositories to suit your needs. The repositories you create are referred to as user-defined repositories.

The following specific terms are used for repository functions.

- **Retrieve Container Files** copies a file from one or more managed hosts to the repository.
- **Upload to Repository** sends a file from your local computer (the computer running the browser) or a network host accessible from your local computer to the repository.
- **Retrieve**  downloads a file from the repository to your local computer network.
- **Upload** copies a file from the repository to one or more managed nodes.

You can perform these operations using repositories:

- Manage logs in the Logs repository
- Manage CA certificates in the CA Certs repository
- Upgrade a connector using an upgrade file available in the Upgrade repository
- Apply a Content ArcSight Update Pack (AUP) on one or more connector
- Maintain centralized repositories of files for connector configuration and management

Logs Repository

When you want to view logs, you need to first **Load** the logs of the container that contains the connector to the Logs repository, and then **Retrieve** the logs to view them.

If a container contains more than one connector, logs for all connectors are retrieved.

For information on loading, retrieving, and deleting the logs, see "Viewing Container Logs" on page 65.

Uploading a File to the Logs Repository

Uploading a file into the Log repository is useful for sharing annotated log or other files with other users. The file needs to be in `.zip` format.

To upload a file:

1. Click **Administration > Repositories.**
2. Click **Logs** from the left panel.
3. Click **Upload** from the management panel.
4. Enter the local file path or click **Browse** to select the file.
5. Click **Submit** to add the specified file to the repository or **Cancel** to quit.

CA Certs Repository

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The CA Certs repository (shown below) enables you to store CA Certs files (that contain one or multiple certificates) and single CA certificates. When certificates are stored in the CA Certs repository, you can add the certificates to a container so that the connectors in the container can validate their configured destinations successfully.

You can add a single certificate to a container that is in FIPS or non-FIPS mode. You can only add a CA Certs file to a container that is in non-FIPS mode.

To associate a CA certificate to a connector, you need to:

- Upload the CA certificate or CA Certs file to the CA Certs repository, as described below.
- Add a CA certificate from the CA Certs repository to the container that contains the connector, as described in "Managing Certificates on a Container" on page 66.

Uploading CA Certificates to the Repository

You can upload a CA Certs file or a single certificate to the CA Certs repository.

Before you upload a single CA certificate, change the name of the certificate on the local computer to a name that you can recognize easily. This helps you distinguish the certificate when it is displayed in the Certificate Management wizard.

To upload certificates to the repository:

1. Click **Administration > Repositories.**
2. Click **CA Certs** in the left panel.
3. Click **Upload** in the management panel.
4. Enter the local path for the CA Certs file or the certificate, or click **Browse** to select it.

Click **Submit** to add the specified CA Certs file or the certificate to the repository, or **Cancel** to quit. The CA Certs Repositories tab shows all the CA Certs files and single certificates that have been uploaded. The Type column shows CERTIFICATE for a single certificate and CACERT for a CA Certs file.

Removing CA Certificates from the Repository

When you delete a CA Certs file or a single certificate from the repository, it is deleted from the system.

When you delete a CA Certs file or a single certificate from the CA Certs repository, containers are not affected; the connectors continue to use the certificates, which are located in a trust store after being added to a container. For information about adding a CA certificate to a container, see "Managing Certificates on a Container" on page 66.

To remove a certificate from the repository:

1. Click **Administration > Repositories.**
2. Click **CA Certs** in the left panel.
3. Identify the certificate or the CA Certs file you want to remove and click its associated **Remove** button ().

Upgrade AUP Repository

The Upgrade AUP repository enables you to maintain a number of connector AUP (upgrade) files. You can apply any of these AUP upgrade files to containers when you need to upgrade to a specific version. As a result, all connectors in a container are upgraded to the version you apply to the container.

This repository can also maintain upgrade files for upgrading remotely-managed Connector Appliances.

About the AUP Upgrade Process

The process discussed in this section only applies to upgrading connectors and to upgrading a remotely-managed Connector Appliance.

To upgrade a connector or to upgrade a remotely-managed Connector Appliance, you need to:

- Upload the appropriate `.aup` upgrade file to the Upgrade AUP repository, as described below.

- Apply the `.aup` upgrade file from the Upgrade AUP repository to the container (see "Upgrading a Container to a Specific Connector Version" on page 176) or to a remote Connector Appliance (see "Upgrading a Host Remotely" on page 161).

Uploading an AUP Upgrade File to the Repository

To upload AUP upgrade files to the repository:

1. Download the upgrade AUP file for the connector or the remote Connector Appliance from the ArcSight Customer Support site at http://support.openview.hp.com/ to the computer that you use to connect to the browser-based interface.
2. From the computer to which you downloaded the upgrade file, log in to the browser-based interface.
3. Click **Administration > Repositories.**
4. Click **Upgrade AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository or click **Cancel** to quit.
8. If you want to apply this upgrade file, follow these instructions:
   - For a container upgrade, see "Upgrading a Container to a Specific Connector Version" on page 176.
   - For a remotely-managed Connector Appliance upgrade, see "Upgrading a Host Remotely" on page 161.

Removing a Connector Upgrade from the Repository

You can remove a connector upgrade file from the repository when you no longer need it. When you remove a connector upgrade file from the repository, it is deleted from the system.

To remove a Connector upgrade from the repository:

1. Click **Administration > Repositories.**
2. Click **Upgrade AUP** from the left panel.
3. Locate the upgrade file that you want to delete and click the associated  icon.

Content AUP Repository

ArcSight continuously develops new connector event categorization mappings, often called *content*. This content is packaged in ArcSight Update Packs (AUP) files. All existing content is included with major product releases, but it is possible to stay completely current by receiving up-to-date, regular content updates through ArcSight announcements and the Customer Support site. The AUP files are located under Content Subscription Downloads.

The ArcSight Content AUP feature enables you to apply an AUP file to applicable connector destinations that you are managing. Only the event categorization information can be applied to the connectors using this feature.

You can maintain a number of Content AUP files in the Content AUP repository. When an AUP file with a version number higher than the ones already in the repository is loaded, it

is automatically pushed out to the connector destinations being managed. However, these connectors or connector destinations are skipped:

- Connectors that are unavailable at the time of the AUP file push
- Connectors whose current version does not fall in the range of versions that the Content AUP supports
- The ESM destination on a connector
- All destinations of a connector that have an ESM destination with the AUP Master flag set to Yes

Also, when a new connector is added, the highest number Content AUP is pushed automatically to its destinations.

Applying a New Content AUP

You can add a new content AUP file to the repository and push it automatically to all applicable managed nodes.

To apply a new Content AUP:

1. Download the new Content AUP version from the support site at http://support.openview.hp.com/ to the computer that you use to connect to the browser-based interface.
2. From the computer to which you downloaded the AUP file, log in to the browser-based interface.
3. Click **Administration > Repositories.**
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository and push it automatically to all applicable connectors, or **Cancel** to quit.

You can verify the current Content AUP version on a connector by performing either of these steps:

- Run the `GetStatus` command on the node destination and check that the value for `aup[acp].version` is the same as the AUP version you applied. For information about running a command on a connector destination, see "Sending a Command to a Connector" on page 82.
- hover over a host name to see the AUP version applied to all destinations of that connector.

Applying an Older Content AUP

If you need to apply an older Content AUP from the Content AUP repository, delete all versions newer than the one you want to apply in the repository. The latest version (of the remaining AUP files) is pushed automatically to all applicable connectors.

To delete a Content AUP from the Content AUP repository:

1. Click **Administration > Repositories.**
2. Click **Content AUP** from the left panel.

3 Locate the AUP file that you want to delete and click the associated  icon. Repeat for multiple files.

User-Defined Repositories

A *user-defined repository* is a user-named collection of settings that control upload and download of particular files from connectors to the repository. Each repository uses a specified path, relative to `$ARCSIGHT_HOME/user/agent`, for files to be uploaded or downloaded. ArcSight connectors use a standard directory structure, so map files, for example, are always found in `$ARCSIGHT_HOME/user/agent`, (that is, the root directory, `$ARCSIGHT_HOME`, of the installation path) in a folder called `map/`.

After they are created, user-defined repositories are listed on the left-side menu, under the **New Repository** heading, and appear with the user-specified display name.

User-defined repositories are expected to be grouped by file type and purpose, such as log files, certificate files, or map files. Each user-defined repository has a name, a display name, and an item display name, which are defined under the **Settings** tab that appears for user- or pre-defined repositories (for details about pre-defined repositories, see "Pre-Defined Repositories" on page 132).

Files viewed in the user-defined repository can be bulk processed with specified hosts and can be exchanged with the user's browser host.

Creating a User-Defined Repository

You can create a new repository at any time.

The repository requires correct directory paths. Your file will be applied to the wrong directory if the entered path contains errors, such as extra spaces or incorrect spellings. You can verify your directory paths by accessing the `Directory.txt` file, which lists the directory structure for every entered path. View the `Directory.txt` file by accessing your container logs and finding the `Directory.txt` file.

To create a new user-defined repository:

1 Click **Administration > Repositories.**

2 Click **New Repository** under the **Repositories** section in the left panel.

3 For the new repository, enter the parameters listed in the following table.

Parameter	Description
Name	A unique name for the repository, typically based on the type of files it contains.
Display Name	The name that will be displayed on the left-side menu and for tabs: Process *names*, View *names*, Settings for *names*. Typically plural.
Item Display Name	The name used to describe a single item.
Recursive	Check to include sub-folders.
Sort Priority	-1 by default

Parameter	Description
Restart Connector Process	Check to restart the connector process after file operations.
Filename Prefix	An identifying word that is included in the names of retrieved files. For example, map files are identified by `Map` in the file name: `localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip`
Relative path (Download)	The path for download, relative to `$ARCSIGHT_HOME`, for example, `user/agent/map` or `user/agent/flexagent`. Leave this field blank to specify files in `$ARCSIGHT_HOME`. **Note**: The relative path is used for download only.
Include Regular Expression	A description of filenames to include. Use `.*` to specify all files. The following example selects properties files that consist of `map`. followed by one or more digits, followed by `.properties`: `map\.[0-9]+\.properties$`
Exclude Regular Expression	A description of filenames to exclude. The following example excludes all files with a certain prefix or in the `agentdata` folder. `(agentdata/|cwsapi_fileset_).*$`
Delete Before Upload	Check to delete earlier copies before upload. **CAUTION**: If you check **Delete Before Upload** and do not specify a Relative path (Upload), all files and folders in `current/user/agent` will be deleted.
Delete Groups	Whether to delete folders recursively in `$ARCSIGHT_HOME/user/agent/map directory`.
Relative path (Upload)	The path for upload, relative to `$ARCSIGHT_HOME/current/user/agent/flexagent/<connectorname>`
Delete Relative Path	Whether the directory specified in **Relative Path (Upload)** and its contents should be removed when a file is uploaded from the repository.
Delete Include Regular Expression	Typically the same as the Include Regular Expression.
Delete Exclude Regular Expression	Typically the same as the Exclude Regular Expression.

4 Click **Save** at the bottom of the page.

The new repository displays under the **New Repository** heading in the left-side window panel.

Retrieving Container Files

The **Retrieve Container Files** button copies a file from one or more containers to a repository. The specific files that are retrieved depend on the settings of the repository.

To retrieve a container file:

1 Click **Administration > Repositories.**

2 In the left panel, under **Repositories**, click the name of the repository to which you want to copy connector files.

3 Click **Retrieve Container Files** in the management panel.

4 Follow the instructions in the Retrieve Container Files wizard.

Uploading Files to a Repository

The upload process copies files from your local computer to a repository.

To upload files to a repository:

1 Click **Administration > Repositories.**

2 In the lower left panel (under **Repositories**), click the name of the repository to which you want to upload files.

3 Click **Upload To Repository** from the management panel.

4 Follow the instructions in the Repository File Creation wizard. Select **Individual files** to create a ZIP file with appropriate path information.

Be sure *not* to change the default sub-folder name `lib` in the **Enter the sub folder where the files will be uploaded** page of the Repository File Creation wizard.

Deleting a Repository

You can delete user-defined repositories only.

To delete a repository:

1 Click **Administration > Repositories.**

2 From the left panel, click the name of the repository you want to delete.

3 Click **Remove Repository** from the management panel.

Updating Repository Settings

The **Settings** tab displays the settings associated with the current repository. An example is shown below. Most settings for pre-defined repositories are read-only; however, you can update settings for user-defined repositories.

To update settings of a repository:

1. Click **Administration > Repositories.**
2. In the left panel, click the name of the repository whose settings you want to update.
3. Click the **Settings for *Repository_Name*** tab from the management panel.
4. Update the settings.
5. Click **Save** at the bottom of the page.

Managing Files in a Repository

You can retrieve files in a repository (download files to your local computer), upload files to a repository, or remove files from a repository.

Connectors require correct properties and proper files. Applying incorrect files, including empty files or files with binary content, can prevent a connector from functioning correctly.

It is possible to upload files with incorrect content, such as an empty `.map` file. The system does not check or warn against such files. To ensure a successful result, only upload known, correct files.

Retrieving a File from the Repository

To retrieve a file from the repository:

1. Click **Administration > Repositories.**

2 From the left panel, click the name of the repository in which the file exists.

3 Click  from the management panel for the file that you want to retrieve.

4 Follow the file download instructions to copy the file to your local computer.

Uploading a File from the Repository

To upload a file from the repository:

1 Click **Administration > Repositories.**

2 In the left panel, click the name of the repository in which the file exists.

3 In the management panel, click **Upload to Repository** for the file that you want to upload.

4 Follow the Upload Container Files wizard instructions to upload the file to the containers of your choice.

5 Verify that the file was uploaded correctly:

- If you have SSH access to the connectors, connect to them and check the file structure.
- Obtain the connector logs and check the contents of the `Directory.txt` file for each connector.

Removing a File from the Repository

To remove a file from the repository:

1 Click **Administration > Repositories.**

2 In the left panel, click the name of the repository in which the file exists.

3 In the management panel, click  for the file that you want to delete.

Pre-Defined Repositories

You can define repositories for any connector-related files. As a convenience, the following repositories are pre-defined.

- **Backup Files**: connector cloning (see "Cloning Container Configuration" on page 136).
- **Map Files**: enrich event data
- **Parser Overrides**: customize the parser (see "Adding Parser Overrides" on page 137)
- **Flex Connector Files**: user-designed connector deployment
- **Connector Properties**: `agent.properties`; subset of cloning
- **JDBC Drivers**: database connectors

To view the settings for a pre-defined repository, click the name of the repository and then click the **Settings** tab in the management panel.

The settings for pre-defined repositories are read-only; to modify the settings, click **New Repository** in the left panel to create a user-defined repository and provide the settings you want to use.

The following tables lists the settings for each pre-defined repository.

Settings for Backup Files

This table lists pre-defined settings for backup files.

Table 10-1 Backup File Settings

Name	Default Setting
Name	backup
Display Name	Backup Files
Item Display Name	Backup File
Recursive	Checked (Yes)
Sort Priority	0
Restart Connector Process	Checked (Yes)
Filename Prefix	ConnectorBackup
Download Relative Path	
Download Include regular expression	
Download Exclude regular expression	(agentdata/|cwsapi_fileset_).*$
Delete before upload	Checked (Yes)
Delete groups	Checked (Yes)
Upload Relative Path	
Delete Relative Path	
Delete Include regular expression	
Delete Exclude regular expression	(agentdata/|cwsapi_fileset_).*$

Settings for Map Files

This table lists pre-defined settings for map files.

Table 10-2 Map File Settings

Name	Default Setting
Name	map
Display Name	Map Files
Item Display Name	Map File
Recursive	Un-checked (No)
Sort Priority	5
Restart Connector Process	Un-checked (No)
Filename Prefix	Map
Download Relative Path	map

Table 10-2 Map File Settings

Name	Default Setting
Download Include regular expression	map\.[0-9]+\.properties$
Download Exclude regular expression	
Delete before upload	Checked (Yes)
Delete groups	Un-checked (No)
Upload Relative Path	
Delete Relative Path	map
Delete Include regular expression	map\.[0-9]+\.properties$
Delete Exclude regular expression	

Settings for Parser Overrides

This table lists pre-defined settings for parser overrides.

Table 10-3 Parser Override Settings

Name	Default Setting
Name	parseroverrides
Display Name	Parser Overrides
Item Display Name	Parser Override
Recursive	Checked (Yes)
Sort Priority	10
Restart Connector Process	Checked (Yes)
Filename Prefix	Parsers
Download Relative Path	fcp
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Checked (Yes)
Delete groups	Checked (Yes)
Upload Relative Path	
Delete Relative Path	fcp
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for FlexConnector Files

This table lists pre-defined settings for FlexConnector files.

Table 10-4 FlexConnector Settings

Name	Default Setting
Name	flexconnectors
Display Name	Flex Connector Files
Item Display Name	Flex Connector File
Recursive	Checked (Yes)
Sort Priority	15
Restart Connector Process	Checked (Yes)
Filename Prefix	FlexConnector
Download Relative Path	flexagent
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Checked (Yes)
Delete groups	Checked (Yes)
Upload Relative Path	
Delete Relative Path	flexagent
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for Connector Properties

This table lists pre-defined settings for Connector Properties.

Table 10-5 Connector Property Settings

Name	Default Setting
Name	connectorproperties
Display Name	Connector Properties
Item Display Name	Connector Property File
Recursive	Un-checked (No)
Sort Priority	20
Restart Connector Process	Checked (Yes)
Filename Prefix	ConnectorProperties
Download Relative Path	
Download Include regular expression	agent\.*
Download Exclude regular expression	

Table 10-5 Connector Property Settings

Name	Default Setting
Delete before upload	Un-checked (No)
Delete groups	Un-checked (No)
Upload Relative Path	
Delete Relative Path	
Delete Include regular expression	agent\.*
Delete Exclude regular expression	

Settings for JDBC Drivers

This table lists pre-defined settings for JDBC Drivers.

Table 10-6 JDBC Driver Settings

Name	Default Setting
Name	jdbcdrivers
Display Name	JDBC Drivers
Item Display Name	Connector JDBC Driver File
Recursive	Un-checked (No)
Sort Priority	25
Restart Connector Process	Checked (Yes)
Filename Prefix	
Download Relative Path	lib
Download Include regular expression	
Download Exclude regular expression	
Delete before upload	Un-checked (No)
Delete groups	Un-checked (No)
Upload Relative Path	
Delete Relative Path	lib
Delete Include regular expression	
Delete Exclude regular expression	

Cloning Container Configuration

Using the **Backup Files** repository, you can quickly copy a container to other containers. As a result, all connectors in the source container are copied to the destination container. This process is called *cloning* a container configuration. You can clone a container to

several containers at once. The contents of the source container replace the existing contents of the destination container.

Do not clone older, software-based connectors (such as build 4.0.8.4964) to containers with newer connector builds (such as 4.0.8.4976 or later).

Cloning a connector using the Backup repository only works if the connector version numbers are the same.

To clone a container:

1. Click **Node Management,** and then click **System** in the left panel.
2. Click the **Containers** tab to list the containers and determine the source and destination for cloning.
3. Click **Administration > Repositories.**
4. Click **Backup Files** under the **Repositories** section in the management panel.
5. If the backup file that you need to use for cloning exists in the repository, go to the next step. Otherwise, follow the instructions in "Retrieving a File from the Repository" on page 131 to retrieve the container's backup file to the Backup repository.

   The retrieved file is named in `<connector name>` ConnectorBackup `<date>` format.
6. Follow the instructions in "Uploading a File from the Repository" on page 132 to upload the backup file to one or more containers.

   The destination containers are unavailable while the backup file is applied and the connectors are restarted.

The backup file does not include the container certificates. You have to re-apply the certificates to the container after you upload the backup file.

After applying the certificates, check the status of the destination container to make sure it is available.

Adding Parser Overrides

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added.

To use parser overrides, you need to:

- Upload a parser override file to the pre-defined **Parser Overrides** repository.
- Download the parser override file to the container that contains the connector that will use the parser override.

Follow the steps below.

To upload a parser override file:

1. Click **Administration > Repositories.**
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. On the **Parser Overrides** tab, click the **Upload To Repository** button.
4. Follow the wizard to upload the file. When prompted by the wizard, make sure you:

- Select the **Individual Files** option from the **Select the type of file that you want to upload** field.
- Add a slash (/) after fcp before adding the folder name in the **Enter the sub folder where the files will be uploaded** field. For example, `fcp/multisqlserver_audit_db`.

When upload is complete, the parser override file is listed in the table on the Parser Overrides tab.

To download the parser override file to a container:

1. Click **Administration > Repositories.**
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. In the table on the **Parser Overrides** tab, locate the parser override file you want to download and click the up arrow next to the file.
4. Follow the wizard to select the container to which you want to add the parser overrides.

   When the wizard completes, the parser overrides are deployed in the selected container.

You can download a parser override file from ArcExchange. For more information, refer to "Sharing Connectors in ArcExchange" on page 86.

To verify that the parser override has been applied successfully, issue a Get Status command to the connector. See "Sending a Command to a Connector" on page 82. In the report that appears, check for the line starting with the text `ContentInputStreamOverrides`.

Chapter 11

System Admin - ArcSight Management Center

This chapter describes the System Administration tools that enable you to create and manage users and user groups, and to configure SMTP and other system settings.

This chapter includes information on the following areas of system administration:

System

From the System tab, you can configure system specific settings such as network settings (if applicable) and SMTP.

SMTP

Your system uses the Simple Mail Transfer Protocol (SMTP) setting to send email notifications such as alerts and password reset emails.

To add or change SMTP settings:

1 Click **Administration > System Admin.**

2 Click **SMTP** in the **System** section and enter these settings.

Setting	Description
Primary SMTP Server	The IP address or hostname of the SMTP server that will process outgoing email.
Backup SMTP Server	The IP address or hostname of the SMTP server that will process outgoing email in case the primary SMTP server is unavailable.
Outgoing Email Address	The email address that will appear in the From: field of outbound email.

3 Click **Save**.

Be sure to configure your reports to use the same SMTP settings. For instructions, see "Backup and Restore of Report Content" on page 200.

License & Update

This page displays license information, the version of the components, and the elapsed time since ArcSight Management Center was last restarted.

Updating the License File

To update a license file:

1 Download the update file from the HP Customer Support site (SSO) at https://support.openview.hp.com to the computer from which you can connect to the ArcSight Management Center with your browser.

2 From the computer to which you downloaded the update file, log in to the ArcSight Management Center user interface using an account with administrator (upgrade) privileges.

3 Click **Administration > System Admin.**

4 Click **License & Update** in the **System** section.

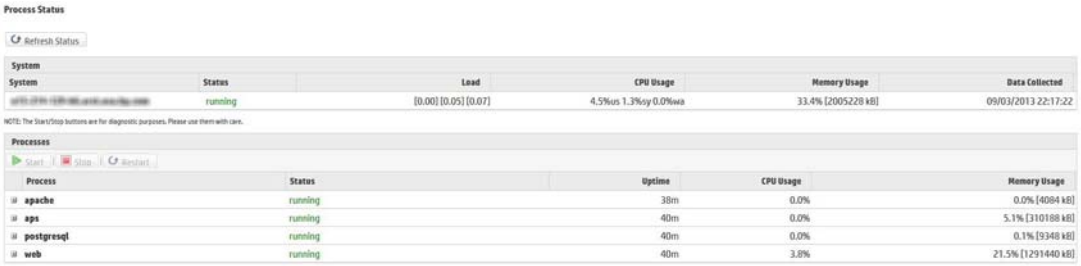
5 Browse to the license file you downloaded earlier, and click **Upload Update**.

An "Update In Progress" page displays the update progress.

After the update has completed, the Update Results page displays the update result (success/failure). If you are only installing or updating a license, a restart is not required.

Process Status

The **Process Status** page lists all processes related to your system and enables you to view the details of those processes and start, stop, or restart them.



To view the Process Status page:

1. Click **Administration > System Admin.**
2. In **System** section, click **Process Status**.
3. To view the details of a process, click the icon to the left of the process name.
4. To start, stop, or restart a process, select the process and click **Start**, **Stop**, or **Restart** at the top of the **Processes** list.

System Settings

If you did not select ArcSight Management Center to start as service during the installation process, you can do so using the **System Settings** page.

To configure ArcSight Management Center to start as a service:

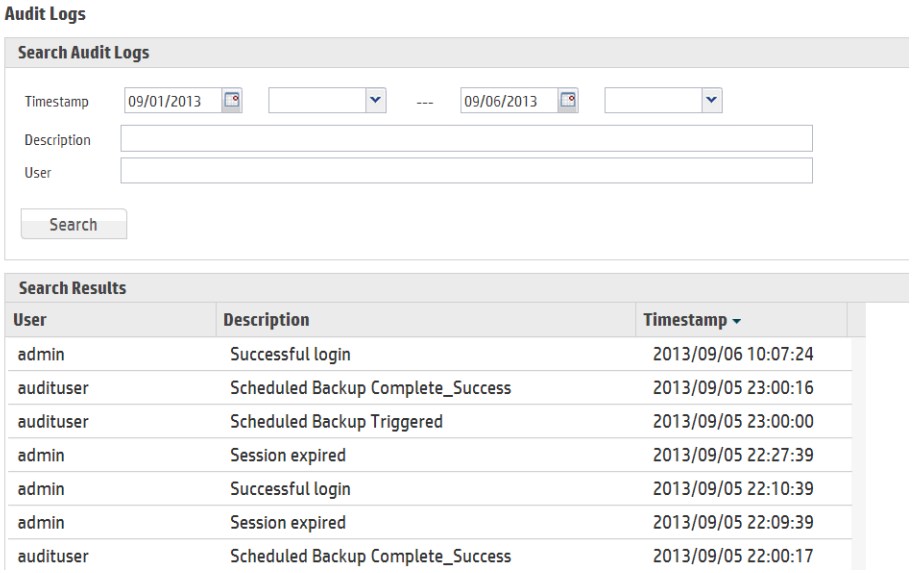
1. Click **Administration > System Admin.**
2. Click **System Settings** in the left panel.
3. From under **Service Settings**, choose the appropriate option:
   - Start as a Service
   - Do not start as a Service
4. Click **Save**.

Logs

Your system can generate audit logs at the application and platform levels. Use the Logs sub-menu to search audit logs.

Audit Logs

Your system's audit logs are available for viewing. Audit logs, as Common Event Format (CEF) audit events, can be sent to ArcSight ESM directly for analysis and correlation.



To view audit logs:

1. Click **Administration > System Admin.**
2. Click **Audit Logs** in the **Logs** section.
3. Select the date and time range for which you want to obtain the log.
4. (Optional) To refine the audit log search, specify a string in the Description field and a user name in the User field. When a string is specified, only logs whose Description field contains the string are displayed. Similarly, when a user is specified, only logs whose User field contains the username are displayed.
5. Click **Search**.

Audit Event Forwarding

To configure ArcSight Management Center to forward application, platform, or system health events, you need to perform the following tasks:

- Upload an ESM certificate to the CA Certs repository
- Add the Syslog Daemon connector to a container
- Set runtime parameters
- Configure on the container.

To configure event forwarding:

1. Upload an ESM certificate to ArcSight Management Center so that the appliance and ArcSight Manager can communicate. To upload the ESM certificate to ArcSight Management Center, refer to “CA Certs Repository” on page 116. (If you already have an ESM certificate in the CA Certs Repository, skip this step.)
2. Add the ESM certificate to a Container. Refer to “Managing Certificates on a Container” on page 178.
3. Add the Syslog Daemon connector to the container to which you added the certificate. Refer to “Adding a Connector” on page 190. (If the syslog connector is already assigned to the container, skip this step.)

4 When choosing a destination, select *ArcSight Manager (encrypted)*.

Security

Security settings enable you to configure SSL server certificates, enable and disable FIPS (Federal Information Processing Standards) mode on your system, and configure SSL client authentication for client certificate and Common Access Card (CAC) support.

For steps on how to create a user DN, see "Users" on page 158, and refer to the section "Use Client DN" in the parameters table.

SSL Server Certificate

Your system uses Secure Sockets Layer (SSL) technology to communicate securely over an encrypted channel with its clients, such as SmartConnectors, when using the SmartMessaging technology and other ArcSight systems. Your system ships with a self-signed certificate so that an SSL session can be established the first time you use the appliance. For more information on this option, see "Generating a Self-Signed Certificate" on page 143.

Although a self-signed certificate is provided for your use, you should use a certificate authority (CA) signed certificate. To facilitate obtaining a CA-signed certificate, your system can generate a Certificate Signing Request. After a signed certificate file is available from the CA, it can be uploaded to your system for use in a subsequent authentication. For detailed instructions, see "Generating a Certificate Signing Request (CSR)" on page 145.

Your system generates an audit event when the installed SSL certificate is going to expire in less than 30 days or has already expired. The event with Device Event Class ID `"platform:407"` is generated periodically until you replace the certificate with one that is not due to expire within 30 days.

Generating a Self-Signed Certificate

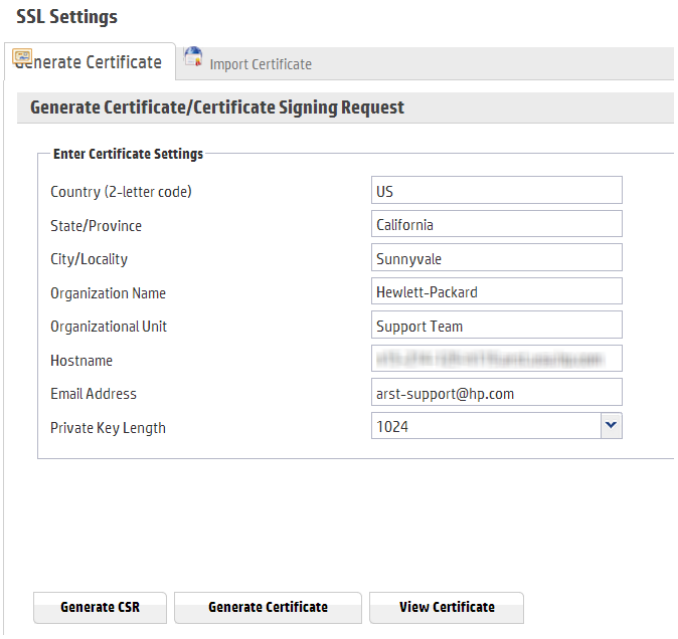
Your system ships with a self-signed certificate so that an SSL session can be established the first time you connect. This type of certificate does not require signing from another entity and can be used immediately.

To generate a self-signed certificate:

1 Click **Administration > System Admin.**

2 Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.

3 Click the **Generate Certificate** tab.



4 From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	ISO 3166-1 two-letter country code, such as 'US' for the United States.
State/Province	State or province name, such as 'California.'
City/Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	The host name or IP address of this system. When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. **Note:** If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	The key length is 2048 bits and may not be changed.

Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

5 Click the **Generate Certificate** button to generate the self-signed certificate.

6 Click **Ok** after the confirmation message appears.

7 Click the **View Certificate** button to view the PEM encoded self-signed certificate.

Generating a Certificate Signing Request (CSR)

The first step in obtaining a CA-signed certificate is to generate a Certificate Signing Request (CSR). The CSR must be generated on the system for which you are requesting a certificate. That is, you cannot generate a CSR for System A on System B or use a third-party utility for generation.

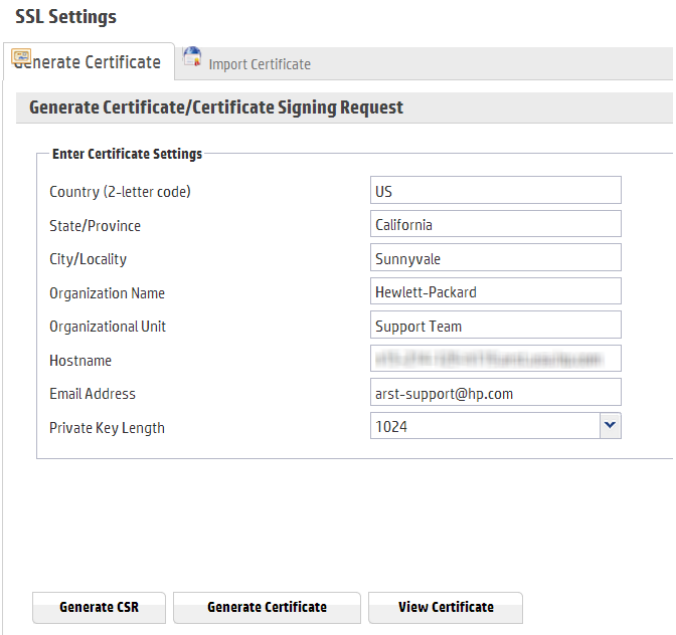
The resulting CSR must be sent to a CA, such as VeriSign, which responds with a signed certificate file.

To generate a certificate signing request:

1 Click **Administration > System Admin.**

2 Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.

3 Click the **Generate Certificate** tab.



4 From the **Enter Certificate Settings** field, enter new values for the following fields:

Parameter	Description
Country	A two-letter country code, such as 'US' for the United States.
State / Province	State or province name, such as 'California.'
City / Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	The host name or IP address of this system. When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. **Note:** If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Select the length (in bits) of the private key: **1024**, **2048**, **4096**, or **8192**.

Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

5 Choose **Generate CSR** to generate a certificate signing request.

6 If the CSR was successfully generated, a pop-up window appears, allowing you to either download the CSR file or to cut-and-paste its content.

To do so, copy all the lines from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----`.

7 Send the CSR file to your certificate authority to obtain the CA-signed certificate.

8 After the CA-signed certificate file is obtained, continue on to Importing a Certificate below.

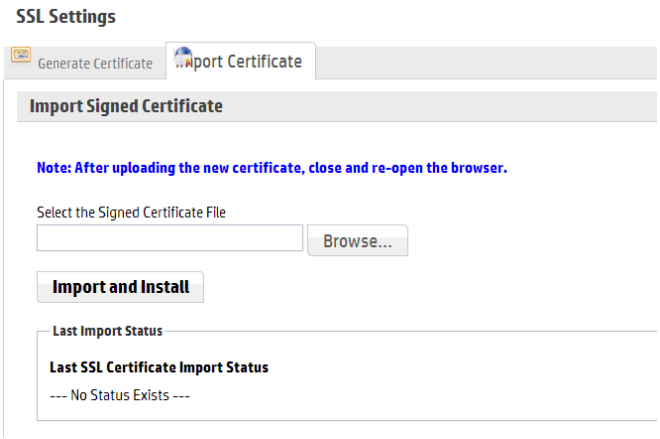
Importing a Certificate

If you have obtained a certificate from your certificate authority (CA), follow the steps below to import it onto your system.

1 Click **Administration > System Admin.**

2 Click **SSL Server Certificate** under the **Security** section in the left panel.

3 Select the **Import Certificate** tab.



4 Click the **Browse** button to locate the signed certificate file on your local file system.

The imported certificate must be in **Privacy Enhanced Mail (PEM)** format.

5 Click **Import and Install** to import the specified certificate.

6 If using **HTTPS** and depending on your browser, you may need to close and restart the browser for the new certificate to take effect. If you are unsure of your browser's requirements, close and restart it.

SSL Client Authentication

Your system supports client authentication using SSL certificates. SSL client authentication is a form of two-factor authentication that can be used as an alternate or in addition to local password authentication. As a result, your system can be configured for SmartCards, such as Common Access Card (CAC) based authentication. CAC is a standard identification card for active duty members of the Uniformed Services, Selected Reserve, DOD civilian employees, and eligible contractor personnel.

CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

To configure Connector Appliance to support CAC, you need to upload a trusted certificate and a certificate revocation list (CRL), and enable client certificate authentication.

Your system also supports LDAP authentication. The SSL certificate for the LDAP server must be uploaded into the trusted store. After uploading the SSL certificate, the aps process must be restarted (**Administration > System Admin > Process Status > aps > Restart**).

Uploading Trusted Certificates

A trusted certificate is used to authenticate users that log in to your system. Uploading a trusted certificate is required if you are using LDAPS authentication. The trusted certificate is used to authenticate the remote LDAPS server. The certificate needs to be in Privacy Enhanced Mail (PEM) format.

To upload a trusted certificate:

1. Click **Administration > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. On the **Trusted Certificates** tab, click **Browse** to find the trusted certificate on your local file system.
4. Click **Upload**.

   The trusted certificate is uploaded and listed in the “Certificates in Repository” list on the same page where you uploaded it.

   To view details about a trusted certificate, click the link displayed in the Certificate Name column.

   To delete a trusted certificate, select the certificate and click **Delete**.

Uploading a Certificate Revocation List

A certificate revocation list (CRL) is a computer-generated record that identifies certificates that have been revoked or suspended before their expiration dates. To support CAC, you need to upload a CRL file to your ArcSight system. The CRL file needs to be in PEM format.

To upload a CRL file:

1. Click **Administration > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. In the **Certificate Revocation List** tab, click **Browse** to find the CRL file on your local file system.
4. Click **Upload**.

   The CRL is uploaded and listed in the Certificate Revocation List.

   To view details about a CRL, click the link displayed in the Issuer Name column.

   To delete a CRL file, select it and click the **Delete** button.

Enabling Client Certificate Authentication

To enable client certificate authentication, see “Client Certificate Authentication” on page 153.

Users/Groups

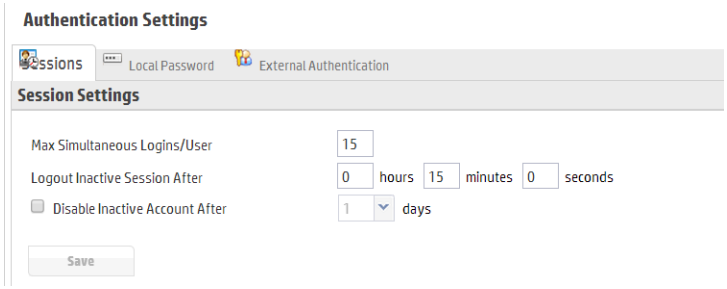
Use the **Users/Groups** sub-menu to configure users and user groups, and to set authentication options.

Authentication

Authentication Settings enable you to specify the settings and policies for user login sessions, password rules and lockouts, and external authentication options.

Sessions

The **Session** tab lets you specify the maximum number of simultaneous sessions for a single user account, and the length of time after which a user session is automatically logged out or a user account disabled. By default, a single user account can have up to 15 simultaneous active sessions, and a user account is logged out after 15 minutes of inactivity.



To change session settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. On the **Sessions** tab, update the parameters described in the following table.

Parameters	Description
Max Simultaneous Logins/User	The maximum number of simultaneous sessions allowed for a single user account. The default is **15 sessions**.
Logout Inactive Session After	The length of time, in minutes, after which an inactive session is automatically ended. The default is **15 minutes**. This value does not apply to the user interface pages accessed through the **Monitor** menu. If a user is on any of the Monitor menu pages and the session has been inactive for the specified number of minutes, the user's session remains active.
Disable Inactive Account After	The number of days after which an inactive user account is disabled. The default is **0**, meaning the account is never disabled.

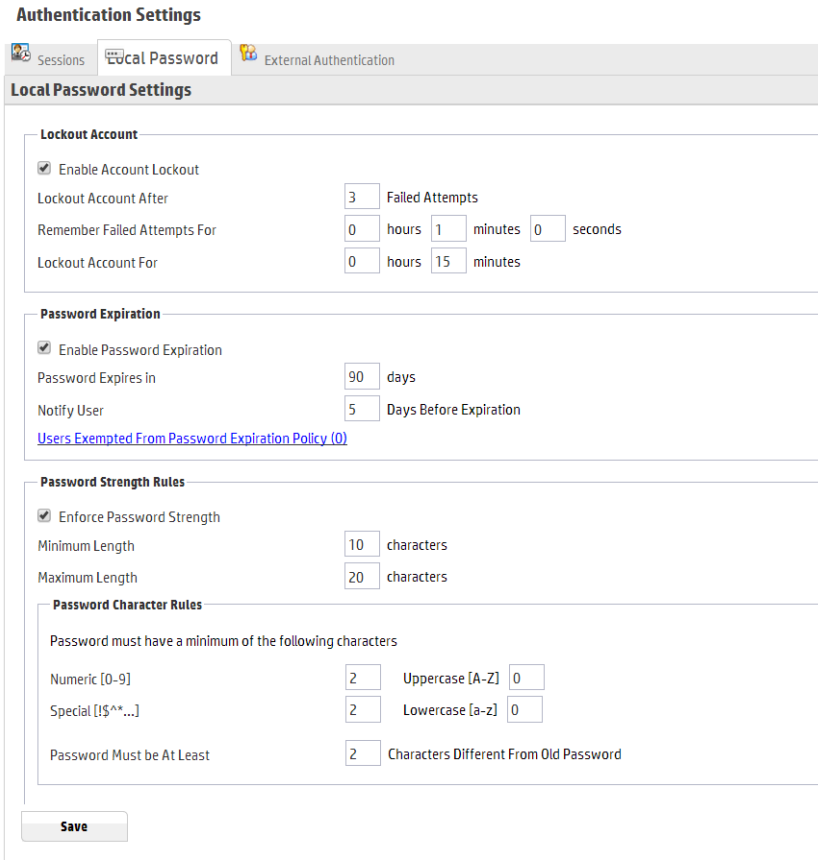
4. Click **Save** to make the changes, or click another tab to cancel.

Local Password

The **Local Password** tab enables you to set password policies, such as the minimum and maximum number of characters and other password requirements.

To change the password settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **Local Password** tab.



Use the parameters described in the following table to customize your password settings.

Table 11-1 Authentication Settings, Local Password tab

Parameter	Description
Lockout Account (policy)	
Enable Account Lockout	Select the checkbox to enable user accounts to be locked out as defined by the following settings. By default, the policy is **disabled**.
Lockout Account After	Number of failed login attempts after which a user account is locked out. The default is **3**.
Remember Failed Attempts For	The length of time, in minutes, for which a failed login attempt is remembered. The default is **1**.

Table 11-1 Authentication Settings, Local Password tab (Continued)

Parameter	Description
Lockout Account For	The length of time, in minutes, for which a locked out account cannot be unlocked. The default is **15**.
Password Expiration (policy)	
Enable Password Expiration	Select the checkbox to enable user passwords to expire as defined by the following settings. By default, the policy is **disabled**.
Password Expires in	Number of days after which the password expires. The default is **90**.
Notify User	Number of days before expiration to notify the user. Select this option to allow users to update their password before expiration. The default is **5**.
Users Exempted From Password Expiration Policy	Click the link to set the number of users whose password should never expire. For information on how to use this feature, see "Users Exempted From Password Expiration" on page 152.
Password Strength Rules (policy)	
Enforce Password Strength	Select the checkbox to enforce password policy as defined by the following settings. By default, the policy is **disabled**.
Minimum Length	Minimum number of characters that a password must contain. The default is **10**.
Maximum Length	Maximum number of characters that a password can contain. The default is **20**.
Password Character Rules	
Password character rules define additional character requirements to ensure password strength.	
Numeric	Minimum number of numeric characters (0-9) in a password. The default is **2**.
Uppercase	Minimum number of uppercase characters (A-Z) in a password. The default is **0**.
Special	Minimum number of non-digit and non-letter characters that are required in a password. The default is **2**.
Lowercase	Minimum number of lowercase characters (a-z) in a password. The default is **0**.
Password Must be At Least N Characters Different From Old Password	Minimum number of characters by which the new password must differ by from the previous one. The default is **2**.

Table 11-1 Authentication Settings, Local Password tab (Continued)

Parameter	Description
Include “Forgot Password” link on Login Screen	Select the checkbox to enable users to reset their local password using a “Forgot Password” link on the login page. By default, the option is **disabled**. An SMTP server must be configured on the system, and the username must have a correct email address for this feature to work successfully. If an SMTP server is not set, you cannot reset the password because the email containing the temporary password cannot be sent. You must specify an email address in the user settings for the user name. The temporary password is sent to that email address. If no email address is specified or if the email address is incorrect, the user will not receive the email. For information on how to use this feature, see “Forgot Password” on page 152.

4 Click **Save** to save the changes, or click another tab to cancel.

Users Exempted From Password Expiration

Even though you have set a password expiration policy for most users, you may want to have a user whose password does not expire automatically.

To exempt a user from the password expiration policy:

1 Click **Administration > System Admin**.

2 Click **Authentication** in the **Users/Groups** section.

3 Choose the **Local Password** tab, and then click **Users Exempted From Password Expiration Policy**.

4 The **Exempt Users From Password Expiration** page displays.

5 Select users from the **Non-exempted Users** list and click the right arrow icon  to move the selected users to the **Exempted Users** list. Do the reverse to remove users from the list of exempted users.

You can select multiple users at the same time and move them over. Or you can move all users by clicking the  icon.

6 Click **Save** to save the policy or **Cancel** to exit.

Forgot Password

This feature is available only if the **Include “Forgot Password” link on Login Screen** setting on the Authentication Settings page (**System Admin > Authentication > Local Password**) is set to **Yes**. By default, this setting is set to **No**. An SMTP server must be configured in order to use this feature. For more details on how to enable it, see “Local Password” on page 150.

If you forget your system password, use this feature to receive an email that provides a temporary password.

The temporary password is valid until the time specified in the email. If you do not log in within the specified time, only an administrator can reset the password to generate another temporary password.

To reset your password:

1. Click the **Forgot Password** link on the Login screen.
2. Enter a user name on the Reset Password dialog box.
3. Click **Reset Password**.

   An automated email with a temporary password is sent to the email address specified for that user.

External Authentication

Besides providing a local password authentication method, your system supports Client Certificate/CAC, LDAP, and RADIUS authentication. It is not possible to enable all authentication methods simultaneously.

CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

From the **External Authentication** tab, use the drop-down menu to choose one of the following authentication methods:

- Local Password
- Client Certificate Authentication
- Client Certificate and Local Password Authentication
- LDAP/AD and LDAPS Authentication
- RADIUS Authentication

Local Password

This option is the default method and implements the local password policies set in the **Local Password** tab. Leave this as the default, or click **Save** if changing from another option.

Client Certificate Authentication

This authentication method requires that users authenticate using a client certificate. For each client certificate, a user account with a Distinguished Name (DN) matching the one in the client certificate must exist on your system.

All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **Client Certificate**.
5. **Allow Local Password Fallback** provides two options:

- **Allow Local Password Fallback for Default Admin Only**

  Select this option to allow the default admin user to log in using only a username and password if the client certificate is not available or invalid. This privilege is restricted to the default admin user only. Other users must have a valid client certificate to gain access to the system. This option is enabled by default.

- **Allow Local Password Fallback for All Users**

  Select this option to allow all users to log in using their local user name and password if their client certificate is invalid or unavailable.

  For more information, see "Local Password Fallback" on page 157.

6 Click **Save**.

Client Certificate and Local Password Authentication

This authentication method requires that users authenticate using an SSL client certificate and a valid local password. *Local Password* refers to the password associated with the user credentials created in **User Management** in the **Users/Groups** section. See "User Management" on page 158 for details.

A user account on your system must be defined with a Distinguished Name (DN) that matches the one in the client certificate.

For instructions on how to create a user DN, see "Users" on page 158 and refer to the section called "Use Client DN" in the parameters table.

All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate and password authentication:

1 Click **Administration > System Admin**.

2 Click **Authentication** in the **Users/Groups** section.

3 Choose the **External Authentication** tab.

4 From the drop-down menu, choose **Client Certificate AND Local Password**.

5 **Allow Local Password Fallback** provides two options:

- **Allow Local Password Fallback for Default Admin Only**

  This option, always enabled, allows the default admin user to log in using only a username and password.

- **Allow Local Password Fallback for All Users**

  This option is always disabled. You cannot enable it when using the **Client Certificate AND Local Password** authentication method.

  For more information, see "Local Password Fallback" on page 157.

6 Click **Save**.

LDAP/AD and LDAPS Authentication

This authentication method authenticates users against an LDAP server. Even when LDAP is enabled, each user account must exist locally on your system. Although the user name specified locally can be different from the one specified on the LDAP server, the

Distinguished Name (DN) specified for each user account must match the one in the LDAP server.

For steps on how to create a user DN, see "Users" on page 158, and the parameter "Use Client DN" on page 159".

To set up LDAP authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **LDAP**.
5. **Allow Local Password Fallback** provides two options:

   - **Allow Local Password Fallback for Default Admin Only**

     Select this option to allow the default admin user to log in using only a username and password if LDAP authentication fails. This privilege is restricted to the default admin user only. All others must be authenticated by LDAP. This option is enabled by default.

   - **Allow Local Password Fallback for All Users**

     Select this option to allow all users to log in using their local user name and password if LDAP authentication fails.

     For more information, see "Local Password Fallback" on page 157.

   LDAP Server has the following parameters:

Parameter	Description

Server Hostname[:port] (optional)	(Optional) Enter the host name or IP address and port of the LDAP server in the following format:
	`ldap://<hostname or IP address>:<port>`
	`ldaps://<hostname or IP address>:<port>`
	Additional steps are required for the use of LDAPS. See Using the LDAP over SSL (LDAPS) Protocol below.

Backup Server Hostname[:Port] (optional)	(Optional) Enter the backup LDAP server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.
Request Timeout	The length of time, in seconds, to wait for a response from the LDAP server. The default is **10**.

6. When finished, click **Save**.

Using the LDAP over SSL (LDAPS) Protocol

When choosing the LDAPS protocol to authenticate users, make sure the following conditions are true:

- The SSL certificate for the LDAPS server has been uploaded into the trusted store.
- The external authentication method is set to "LDAP".
- The URL for the LDAPS server(s) starts with "ldaps://".

After uploading the SSL certificate, restart the **aps** process (**Setup > System Admin > Process Status > aps Restart**).

If the aps process is not restarted, attempts to authenticate using LDAPS will fail.

RADIUS Authentication

This authentication method allows users to authenticate against a RADIUS server. Even when RADIUS authentication is enabled, each user account must exist locally on your system. The username must match the one in the RADIUS server, although the password can be different. A user must present a valid username and (RADIUS) password to be successfully authenticated.

To configure RADIUS authentication settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **External Authentication** tab.
4. From the drop-down menu, choose **RADIUS.**
5. **Allow Local Password Fallback** provides two options:
   - **Allow Local Password Fallback for Default Admin Only**

     Select this option to allow the default admin user to log in using only a username and password if RADIUS authentication fails. This privilege is restricted to the admin user only. All others must be authenticated by RADIUS. This option is enabled by default.
   - **Allow Local Password Fallback for All Users**

     Select this option to allow all users to log in using their local user name and password, if RADIUS authentication fails. For more information, see "Local Password Fallback" on page 157.
6. **Update the RADIUS Server** parameters as necessary:

Parameter	Description
Server Hostname[:port]	Enter the host name and port of the RADIUS server.
Backup Server hostname[:port] (optional)	**(Optional)** Enter the backup RADIUS server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.

Parameter	Description
Shared Authentication Secret	Enter a RADIUS passphrase.
NAS IP Address	The IP address of the Network Access Server (NAS).
Request Timeout	The length of time, in seconds, to wait for a response from the RADIUS server (in seconds). The default is **10**.
Retry Request	Number of times to retry a RADIUS request. The default is **1**.
RADIUS Protocol:	Use the drop-down menu to choose a protocol option. The default is **None**.

7 Click **Save**.

Local Password Fallback

You can use this feature to log in using your local user name and password if the external authentication (Certificate, LDAP, or RADIUS) fails, if you forgot your password to the authentication server, or if the authentication server is not available.

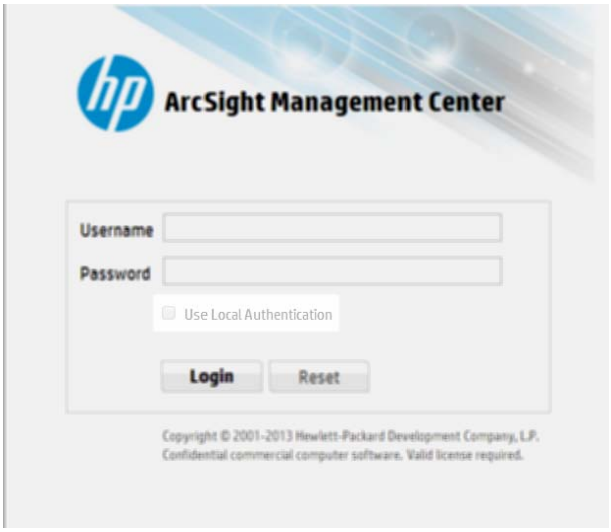
The Use Local Authentication allows the default admin to log in even when the remote authentication server is not available, by adding a **Use Local Authentication** checkbox to the login screen. Out-of-box, this option is enabled only for the default administrator. However, it is possible to allow local password fallback for all users. For example, you could configure the RADIUS authentication method to allow users to log in using local authentication instead of RADIUS should they fail to authenticate to the configured external RADIUS server(s).

For information on how to allow local password fallback for all users for all users, see "Client Certificate Authentication" on page 153, "LDAP/AD and LDAPS Authentication" on page 154, or "RADIUS Authentication" on page 156.

To log in when authentication fails:

1 Mark the **Use Local Authentication** checkbox if the login failure was caused by failure of the external authentication.

This option is only available to the default admin unless it has been enabled for other users.



2 Enter your login and password and click **Login**.

Login Banner

You can customize the message on the login screen to suit your needs. The text you enter in the Content field is displayed above the Username and Password fields on the login screen. In addition, you can enter a confirmation message that the user must click to enable the Username and Password fields.

You must have the “Configure Login Settings” permission enabled for your user account to edit the login banner.

To customize the login banner:

1 Click **Administration > System Admin**.

2 Click **Login Banner** in the **Users/Groups** section.

3 Enter the text you want to display as the login banner in the **Content** field.

You can enter only unformatted text in this field; however, you can apply standard HTML tags to display formatted text. Loading images in this field is not allowed.

4 (Optional) Enter text in the **Confirmation** field. Any text entered will be displayed in the login banner, accompanied by a check box that the user must click to enable the **Username** and **Password** fields. For example, if you enter “Are you sure?”, then the user must click the checkbox in order to confirm log in.

5 Click **Save**.

User Management

The **Users** and **Groups** tabs enable you to manage users and user groups on your system. User groups are a way to enforce access control to various sections of your system.

Users

Open the **Users** tab to manage the users that can log in to your system. You can add a new user, edit user information, or delete a user at any time. You must have the appropriate System Admin group rights to perform these functions.

To add a new user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, click **Add** from the top left side of the page.
4. Enter the following parameters.

Parameter	Description
Credentials	
Login	The user's login name.
Password	The user's password.
Confirm Password	Reenter the users' password.
Contact Information	

Use Client DN	If you enabled SSL client certificate or LDAP authentication, click this link to enter user's the Distinguished Name (Certificate Subject) information. The Distinguished Name should be similar to this format:
	`CN=UserA,OU=Engg Team,O=ArcSight\, Inc.,L=Cupertino,C=US,ST=California`
	To determine the DN, use this URL to display the certificate:
	`https://<hostname or IP address>/platform-service/DisplayCertificate`
	OR
	Obtain the DN information for a user from the browser that the user will open to connect to the system. For example, on Mozilla Firefox, click **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates** > **Your Certificates** > ***Select the certificate*** > **View**.

First Name	The user's first name.
Last Name	The user's last name.
Email	The user's email address.
Phone Number	(Optional) The user's phone number.
Title	(Optional) The user's title.
Department	(Optional) The user's department.
Fax	(Optional) The user's fax number.
Alternate Number	(Optional) The user's alternate phone number.
Assign to Groups	Select the groups to which this user belongs. This setting controls the privileges a user has on this ArcSight Management Center.
System Admin	• Select **Default System Admin Group** to give the user rights to change the settings in the System Admin menu. Choosing this option displays all the tabs and menus. • Select **Read Only System Admin Group** to allow read-only access.

Parameter	Description
ArcMC Rights	• Select **Default ArcMC Rights Group** to give the user rights to the **Monitor** and **Manage** tabs, as well as the **Backup/Restore** and **Repositories** menus. Choosing this option displays all the tabs and menus. • Select **Read Only ArcMC Group** to allow read-only access. • Select Unassigned
Notes	(Optional) Other information about the user.

5 Click **Save and Close**.

To edit a user:

1 Click **Administration > System Admin.**

2 Click **User Management** in the **Users/Groups** section in the left panel.

3 In the **Users** tab, select the user (or users) you want to edit.

4 Click **Edit** from the top left side of the page.

5 Update the user information as necessary.

6 Click **Save User**.

To delete a user:

1 Click **Administration > System Admin.**

2 Click **User Management** in the **Users/Groups** section in the left panel.

3 In the **Users** tab, select the user (or users) you want to delete.

4 Click **Delete** from the top left side of the page.

Reset Password

The Reset Password feature enables you to reset a user's password without knowing their password. If you are using an SMTP-configured server and have permissions to create and update users, you can reset a user's password by clicking the **Reset Password** button. An automated email including the new password string is sent to the user.

An SMTP server must be configured for the automated email containing the temporary password to be sent. If an SMTP server is not configured, the password will not be reset because an email cannot be sent.

To reset a user's password:

1 Click **Administration > System Admin.**

2 Click **User Management** in the **Users/Groups** section in the left panel.

3 In the **Users** tab, select the user (or users) whose passwords you want to reset.

4 Click **Reset Password** from the top left side of the page.

The user must use the temporary string to log in within the time specified in the email. If the user does not log in within the specified time, the account becomes deactivated. If the account has been deactivated, the admin must re-activate it before resetting the password.

To activate a user:

1. Click **Administration > System Admin.**
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) that you want to activate.
4. Choose **Edit**.
5. Check the **Active** box.
6. **Save** the changes.

Groups

User groups define privileges to specific functions on your system and serve to enforce access control to these functions. For example, if you want User A to perform system admin related activities that are not Connector Appliance management specific, assign that user to the System Admin group, but not to the Connector Appliance group.

User groups are divided into the following types: System Admin and Connector Appliance Rights Groups. Each type has a pre-defined, default user group in which all privileges for the type are enabled. To authorize a subset of the privileges for a specific group type, create a new user group and enable only the privileges you want to provide for that group. Then, assign restricted users to the newly created group.

System Admin Groups

System Admin Group

The System Admin Group controls the system administration operations for your system, such as configuring network information, setting storage mounts, installing SSL certificates, and user management.

Read Only System Admin Group

In addition to the default System Admin Group that enables all rights (privileges), a Read Only System Admin Group is available on your system. Users assigned to this group can view System Admin settings, but cannot change them.

ArcSight Management Center Rights Groups for ArcSight Management Center

ArcSight Management Center Rights Group

The Connector Appliance Rights Group controls the ArcSight Management Center application operations for your system, such as viewing the ArcSight Management Center dashboards and backup operations.

Read Only ArcSight Management Center Group

In addition to the default Connector Appliance Rights Group that enables all rights (privileges), Connector Appliance provides more controlled authorizations and a “view only” default option. A read-only user can view the tabs and the operations displayed on the tabs, and can perform operations such as refresh, view certificate list, and Logfu.

Refer to your system’s user interface for a complete list of rights available to this group.

Managing a User Group

To create a new user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Click **Add** from the top left side of the page.
5. Define the new group:
   a. In the **Group Name** field, provide a name for the group.
   b. In the **Description** field, provide a description for the group.
   c. From the Group Type drop-down box, select the group type.
   d. Click the down arrow icon ( ) next to the group type name to view and select privileges that you want to assign to the users in this group.
6. Click **Save and Close** to save the settings of the group, or click **Save and Edit Membership** to add users to this group.

To edit a user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group that you want to edit, and click **Edit** at the top left side of the page.
5. Update the user group information.

   If you need to edit the group's membership:

   a. Click **Save and Edit Membership** to display the Edit Group Membership page.
   b. Click **Add** from the top left of the Edit Group Membership page.
   c. Select users you want to add. By default, you can add only users who do not belong to other groups of the type that you are editing. To add such users, click **Show users that belong to other <group_type> groups**.

      When you add a user who belongs to another group of the same group type as the one you are updating, that user is automatically removed from the previous group.
   d. Click **OK**.
   e. Click **Back to Group List**.
6. Click **Save and Close**.

To delete a user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group (or groups) that you want to delete.

5 Click **Delete** at the top left side of the page.

Change Password

You can use the **Change Password** menu to change your password. Passwords are subject to the password policy specified by the Admin user.

To change your password:

1 Click **Administration > System Admin**.

2 Click **Change Password** in the **Users/Groups** section in the left panel to display the Change Password for <User Name> page.

3 Enter the Old Password, the New Password, and enter the New Password a second time to confirm.

4 Click **Change Password**.

Appendix A
Audit Logs

The following topics are discussed here.

Audit Event Types

You can forward ArcSight Management Center audit events, which are in Common Event Format (CEF), to a destination of your choice.

Several types of audit events are generated by ArcSight Management Center:

- **Application events:** related to ArcSight Management Center functions and configuration changes
- **Platform events:** related to the ArcSight Management Center system
- **System health events:** related to ArcSight Management Center health.

Audit Event Information

An ArcSight Management Center audit event contains information about the following prefix fields.

- Device Event Class ID
- Device Severity
- Name
- Device Event Category (`cat`)

See "Audit Logs" on page 141 for details on how to generate audit logs.

Application Events

Table A-1 Application Events

Signature	Severity	Description	Category
Connector			
connector:101	1	Connector add successful	/Connector/Add/Success
connector:102	1	Connector deleted	/Connector/Delete
connector:103	1	Connector parameters update successful	/Connector/Parameter/Update/Success
connector:201	1	Connector add failed	/Connector/Add/Fail
connector:202	1	Connector delete failed	/Connector/Delete/Fail
connector:203	1	Connector parameters update failed	/Connector/Parameter/Update/Fail
ArcSight Management Center			
arcmc:101	1	ConfigurationBackupScheduler add successful	/BackupScheduler/Add/Success
arcmc:102	1	ConfigurationBackupScheduler update successful	/BackupScheduler/Update/Success
arcmc:103	1	ConfigurationBackupScheduler delete successful	/BackupScheduler/Delete/Success
arcmc:104	1	Scheduled Backup triggered	/Backup/Scheduled/Trigger
arcmc:105	1	Scheduled Backup completed	/Backup/SScheduled/Complete/Success
arcmc:106	1	Manual Backup completed	/Backup/Manual/Complete/Success
arcmc:107	1	Local Backup completed	/Backup/Local/Complete/Success
arcmc:108	1	You have exceeded the maximum number of managed connectors allowed by your license.	/RemotelyManagedConnectors/Exceeded
arcmc:110	1	You have exceeded the maximum number of managed products allowed by your license.	/managedproducts/exceeded
arcmc:112	1	New configuration created successfully.	/Configuration/Add/Success
arcmc:114	1	Delete configurations successful.	/Configuration/Delete/Success

Table A-1 Application Events

Signature	Severity	Description	Category
arcmc:115	1	Push configuration successful.	/Configuration/Push/Success
arcmc:116	1	Import configuration successful.	/Configuration/Import/Success
arcmc:117	1	Add subscriber to configuration successful.	/Configuration/Subscribe/ Success
arcmc:118	1	Unsubscribe node for configuration successful.	/Configuration/Unsubscribe/ Success
arcmc:119	1	Check compliance of configuration successful.	/Configuration/Check Compliance/Success
arcmc:120	1	Configuration set successful.	/Node/Set/Configuration/ Success
arcmc:121	1	Configuration appended successfully.	/Node/Append/Configuration/ Success
arcmc:201	1	ConfigurationBackupScheduler add failed	/BackupScheduler/Add/Fail
arcmc:202	1	ConfigurationBackupScheduler update failed	/BackupScheduler/Update/Fail
arcmc:203	1	ConfigurationBackupScheduler delete failed	/BackupScheduler/Delete/Fail
arcmc:205	1	Scheduled Backup failed	/Backup/Scheduled/Complete/ Fail
arcmc:206	1	Manual Backup failed	/Backup/Manual/Complete/Fail
arcmc:212	1	New configuration creation failed.	/Configuration/Add/Fail
arcmc:213	1	Edit configuration failed.	/Configuration/Update/Fail
arcmc:214	1	Configuration deletion failed.	/Configuration/Delete/Fail
arcmc:215	1	Import configuration failed.	/Configuration/Import/Fail
arcmc:216	1	Push configuration failed.	/Backup/Local/Push/Fail
arcmc:217	1	Add subscriber to configuration failed.	/Configuration/Subscribe/Fail
arcmc:218	1	Unsubscribe node for configuration failed.	/Configuration/Unsubscribe/Fail
arcmc:219	1	Check compliance of configuration failed.	/Configuration/Check Compliance/Success
arcmc:220	1	Configuration set failed.	/Node/Set/Configuration/ Fail

Table A-1 Application Events

Signature	Severity	Description	Category
arcmc:221	1	Configuration append failed.	/Node/Append/Configuration/Fail
arcmc:222	1	Agent install success.	/ArcMCAgent/Install/Success
arcmc:223	1	Agent install failed.	/ArcMCAgent/Install/Failure
Destination			
destination:102	1	Destination update to a connector successful	/Connector/Destination/Update/Success
destination:103	1	Destination delete from a connector successful	/Connector/Destination/Delete/Success
destination:104	1	Destination configuration update successful	/Connector/Destination/Configuration/Update/Success
destination:105	1	Register destination successful	/Connector/Destination/Registration/Success
destination:106	1	Destination configuration add successful	/Connector/Destination/Configuration/Add/Success
destination:107	1	Destination configuration delete successful	/Connector/Destination/Configuration/Delete/Success
destination:202	1	Destination update to a connector failed	/Connector/Destination/Update/Fail
destination:203	1	Destination delete from a connector failed	/Connector/Destination/Delete/Fail
destination:204	1	Destination configuration update failed	/Connector/Destination/Configuration/Update/Fail
destination:205	1	Register destination failed	/Connector/Destination/Registration/Fail
destination:206	1	Destination configuration add failed	/Connector/Destination/Configuration/Add/Fail
destination:207	1	Destination configuration delete failed	/Connector/Destination/Configuration/Delete/Fail
Container			
container:101	1	Container upgrade successful	/Container/Upgrade/Success
container:102	1	User file push to a container successful	/Container/UserFiles/Push/Success
container:103	1	User file delete from container	/Container/UserFiles/Delete
container:104	1	CA cert push to a container successful	/Container/CACert/Push/Success

Table A-1 Application Events

Signature	Severity	Description	Category
container:105	1	Enable demo CA for a container successful	/Container/DemoCA/Enable/Success
container:106	1	Disable demo CA for a container successful	/Container/DemoCA/Disable/Success
container:109	1	Delete property from a container successful	/Container/Property/Delete/Success
container:110	1	Update property to a container	/Container/Property/Update/Success
container:111	1	Container password update successful	/Container/Password/Update/Success
container:112	1	Container add successful	/Container/Add/Success
container:113	1	Container update	/Container/Update
container:114	1	Container delete	/Container/Delete
container:115	1	Add certificate for a container successful	/Container/Certificate/Add/Success
container:116	1	Delete certificate for a container successful	/Container/Certificate/Delete/Success
container:117	1	Enable FIPS on a container successful	/Container/FIPS/Enable/Success
container:118	1	Disable FIPS on a container successful	/Container/FIPS/Disable/Success
container:119	1	Upgrade was triggered for container that resides on end of life appliance model	Container/FromEndOfLifeModel/Upgrade/Triggered
container:201	1	Container upgrade failed	/Container/Upgrade/Fail
container:202	1	User file push to a container failed	/Container/UserFiles/Push/Fail
container:204	1	CA cert push to a container failed	/Container/CACert/Push/Fail
container:205	1	Enable demo CA for a container failed	/Container/DemoCA/Enable/Fail
container:206	1	Disable demo CA for a container failed	/Container/DemoCA/Disable/Fail
container:209	1	Delete property from a container failed	/Container/Property/Delete/Fail
container:210	1	Update property to a container failed	/Container/Property/Update/Fail
container:211	1	Container password update failed	/Container/Password/Update/Fail
container:212	1	Container add failed	/Container/Add/Fail

Table A-1 Application Events

Signature	Severity	Description	Category
container:215	1	Add certificate for a container failed	/Container/Certificate/Add/Fail
container:216	1	Delete certificate for a container failed	/Container/Certificate/Delete/ Fail
container:217	1	Enable FIPS on a container failed	/Container/FIPS/Enable/Fail
container:218	1	Disable FIPS on a container failed	/Container/FIPS/Disable/Fail
container:301	1	Container upgrade started	/Container/Upgrade/Start
Location			
location:101	1	Location add successful	/Location/Add/Success
location:102	1	Location update	/Location/Update
location:103	1	Location delete	/Location/Delete
location:201	1	Location add failed	/Location/Add/Fail
Host			
host:101	1	Host add successful	/Host/Add/Success
host:103	1	Host delete	/Host/Delete
host:105	1	Host certificate download and import successful	/Host/Certificate/Download /Import/Success
host:201	1	Host add failed	/Host/Add/Fail
host:205	1	Host certificate download and import faied	/Host/Certificate/Download Import/Fail

Platform Events

Table A-2 Platform Events

Signature	Severity	Definition	Category
platform:200	7	Failed password change	/Platform/Authentication/PasswordChange/Failure
platform:201	7	Failed login attempt	/Platform/Authentication/Failure/Login
platform:202	5	Password changed	/Platform/Authentication/Password
platform:203	7	Login attempt by inactive user	/Platform/Authentication/InactiveUser/Failure
platform:213	7	Audit forwarding modified	/Platform/Configuration/Global/AuditEvents
platform:220	5	Installed certificate	/Platform/Certificate/Install
platform:221	7	Certificate mismatch failure	/Platform/Certificate/Mismatch
platform:222	1	Created certificate signing request	/Platform/Certificate/Request
platform:224	5	Re-generate self-signed certificate	/Platform/Certificate/Regenerate
platform:226	7	Uploaded update file damaged or corrupt	/Platform/Update/Failure/CorruptPackage
platform:227	5	Update installation success	/Platform/Update/Applied
platform:228	7	Update installation failure	/Platform/Update/Failure/Installation
platform:230	5	Successful login	/Platform/Authentication/Login
platform:234	7	Failed login attempt (LOCKED)	/Platform/Authentication/Failure/LOCKED
platform:239	1	User logout	/Platform/Authentication/Logout
platform:240	3	Added user group	/Platform/Groups/Add
platform:241	3	Updated user group	/Platform/Groups/Update
platform:242	5	Removed all members from group	/Platform/Authorization/Groups/Membership/Update/Clear
platform:244	3	Deleted user group	/Platform/Groups/Remove
platform:245	3	Added user	/Platform/Users/Add
platform:246	3	Updated user	/Platform/Users/Update
platform:247	3	Deleted user	/Platform/Users/Delete
platform:248	3	Session expired	/Platform/Authentication/Logout/SessionExpiration
platform:249	7	Account locked	/Platform/Authentication/AccountLocked

Table A-2 Platform Events

Signature	Severity	Definition	Category
platform:262	5	Appliance time modified	/Platform/Configuration/Time
platform:267	5	SMTP settings modified	/Platform/Configuration/SMTP
platform:269	5	Updated Platform Settings	/Platform/Configuration
platform:270	9	Stopped process '<process>'	/Platform/Process/Control/Stop
platform:280	7	Appliance reboot initiated	/Appliance/State/Reboot/Initiate
platform:281	3	Appliance reboot canceled	/Appliance/State/Reboot/Cancel
platform:282	9	Appliance poweroff initiated	/Appliance/State/Shutdown
platform:300	5	Installed trusted certificate	/Platform/Certificate/Install
platform:301	5	Installed certificate revocation list	/Platform/Certificate/Revocation/ Install
platform:302	5	Deleted trusted certificate	/Platform/Certificate/Delete
platform:303	5	Deleted certificate revocation list	/Platform/Certificate/Revocation/ Delete
platform:304	7	Failed installing trusted certificate	/Platform/Certificate/Install/Failure
platform:305	7	Failed installing certificate revocation list	/Platform/Certificate/Revocation/ Install/Failure
platform:306	5	Start process	/Platform/Process/Start
platform:307	5	Stop process	/Platform/Process/Stop
platform:308	5	Restart process	/Platform/Process/Restart
platform:310	5	Enabled FIPS mode	/Platform/Configuration/FIPS/Enable
platform:311	7	Disabled FIPS mode	/Platform/Configuration/FIPS/Disable
platform:320	3	Appliance poweroff canceled	/Appliance/State/Shutdown/Cancel
platform:371	5	Restarted OS service	/Platform/Service/Restart
platform:400	1	Ran diagnostic command	/Platform/Diagnostics/Command
platform:407	7	SSL certificate expiration warning	/Platform/Certificate/SSL/Expiration
platform:408	5	Appliance startup completed	/Appliance/State/Startup
platform:409	3	Configure login warning banner	/Platform/Configuration/LoginBanner
platform:440	3	SNMP configuration modified	Platform/Configuration/SNMP
platform:500	5	Remove member from group	/Platform/Authorization/Groups/ Membership/Remove

Table A-2 Platform Events

Signature	Severity	Definition	Category
platform:501	5	Group member added	/Platform/Authorization/Groups/Membership/Add
platform:502	5	User removed from group	/Platform/Authorization/Users/Groups/Remove
platform:503	5	User added to group	/Platform/Authorization/Users/Groups/Add
platform:530	5	Authentication Session settings successfully changed	/Platform/Configuration/Authentication/Sessions/Success
platform:540	5	Password Lockout settings successfully updated	/Platform/Configuration/Authentication/Password/Lockout/Success
platform:550	5	Password Expiration settings successfully changed	/Platform/Configuration/Authentication/Password/Expiration/Success
platform:560	5	Password Validation settings successfully changed	/Platform/Configuration/Authentication/Password/Validation/Success
platform:570	5	Allow Automated Password Reset settings successfully changed	/Platform/Configuration/Authentication/Password/AutomatedReset/Success
platform:590	5	RADIUS authentication settings successfully changed	/Platform/Configuration/Authentication/RADIUS/Success
platform:600	5	LDAP authentication settings successfully changed	/Platform/Configuration/Authentication/LDAP/Success
platform:610	5	Global authentication settings successfully changed	/Platform/Configuration/Authentication/Global/Success

System Health Events

System health events provide four status indicators:

- OK
- Degraded
- Rebuilding
- Failed

An **OK** event, indicating normal system behavior, is generated once every ten minutes (six events per hour, per sensor). For a status other than **OK** (**Degraded**, **Rebuilding**, or **Failed**), the event is sent every minute until the sensor returns an **OK** status.

SNMP Related Properties

The following list provides the event fields for system health events sent via SNMP traps. For detailed instructions on setting up SNMP traps, see Chapter 5, SNMP, on page 56.

- event.deviceReceiptTime
- event.deviceVendor
- event.deviceVersion
- event.name
- event.deviceEventCategory
- event.deviceCustomNumber1Label
- event.deviceCustomString1Label
- event.deviceCustomString2Label
- event.deviceCustomString3Label
- event.deviceCustomString4Label
- event.deviceCustomString5Label
- event.deviceCustomString6Label
- event.deviceAddress
- event.endTime
- event.deviceProduct
- event.deviceEventClassId
- event.deviceSeverity
- event.deviceCustomNumber1
- event.deviceCustomString1
- event.deviceCustomString2
- event.deviceCustomString3
- event.deviceCustomString4
- event.deviceCustomString5
- event.deviceCustomString6
- event.destinationAddress

The **snmp.mib.version** is set to 5.0.

Table A-3 System Health Events

Signature	Severity	Definition	Category
CPU			
cpu:100	1	Global health statistics for the CPUs	/Monitor/CPU/Usage
cpu:101	1	Health statistics per CPU	/Monitor/CPU*n*/Usage
Disk			
disk:101	1	Root Disk Space Remaining	/Monitor/Disk/Space/Remaining/Data
disk:102	1	Health statistics per disk (read)	/Monitor/Disk/*drive*/Read
disk:103	1	Health statistics per disk (write)	/Monitor/Disk/*drive*/Write
disk:104	1	Disk Space Remaining	/Monitor/Disk/Space/Remaining/Root
Hardware			
hardware:101	1	Electrical (Current) OK	/Monitor/Sensor/Current/Ok**
hardware:102	5	Electrical (Current) Degraded	/Monitor/Sensor/Current/Degraded**

Table A-3 System Health Events

Signature	Severity	Definition	Category
hardware:103	8	Electrical (Current) Failed	/Monitor/Sensor/Current/Failed**
hardware:111	1	Electrical (Voltage) OK	/Monitor/Sensor/Voltage/Ok**
hardware:112	1	Electrical (Voltage) Degraded	/Monitor/Sensor/Voltage/Degraded**
hardware:113	1	Electrical (Voltage) Failed	/Monitor/Sensor/Voltage/Failed**
hardware:121	1	Battery OK	/Monitor/Sensor/Battery/Ok**
hardware:122	5	Battery Degraded	/Monitor/Sensor/Battery/Degraded **
hardware:123	8	Battery Failed	/Monitor/Sensor/Battery/Failed**
hardware:131	1	Fan OK	/Monitor/Sensor/Fan/Ok
hardware:132	5	Fan Degraded	/Monitor/Sensor/Fan/Degraded
hardware:133	8	Fan Failed	/Monitor/Sensor/Fan/Failed
hardware:141	1	Power Supply OK	/Monitor/Sensor/PowerSupply/Ok
hardware:142	5	Power Supply Degraded	/Monitor/Sensor/PowerSupply/ Degraded
hardware:143	8	Power Supply Failed	/Monitor/Sensor/PowerSupply/Failed
hardware:151	1	Temperature OK	/Monitor/Sensor/Temperature/Ok
hardware:152	1	Temperature Degraded	/Monitor/Sensor/Temperature/ Degraded
hardware:153	1	Temperature Failed	/Monitor/Sensor/Temperature/Failed
Memory			
memory:100	1	Health statistics for platform memory	/Monitor/Memory/Usage/Platform
memory:101	1	Health statistics for JVM memory	/Monitor/Memory/Usage/Jvm
memory:102	1	Health statistics for platform buffers memory	/Monitor/Memory/Usage/Platform/ Buffers
memory:103	1	Health statistics for platform cached memory	/Monitor/Memory/Usage/Platform/ Cached
memory:104	1	Health statistics for platform free memory	/Monitor/Memory/Usage/Platform/ Free
memory:105	1	Health statistics for JVM heap memory	/Monitor/Memory/Usage/Jvm/Heap
memory:106	1	Health statistics for JVM non-heap memory	/Monitor/Memory/Usage/Jvm/ NonHeap
Network			

Table A-3 System Health Events

Signature	Severity	Definition	Category
network:100	1	Health statistics per network interface (input)	/Monitor/Network/Usage/*iface*/In
network:101	1	Health statistics per network interface (output)	/Monitor/Network/Usage/*iface*/Out
RAID			
raid:101	1	RAID Controller OK	/Monitor/RAID/Controller/OK
raid:102	5	RAID Controller Degraded	/Monitor/RAID/Controller/Degraded
raid:103	8	RAID Controller Failed	/Monitor/RAID/Controller/Failed
raid:111	1	RAID BBU OK	/Monitor/RAID/BBU/Ok
raid:112	5	RAID BBU Degraded	/Monitor/RAID/BBU/Degraded
raid:113	8	RAID BBU Failed	/Monitor/RAID/BBU/Failed
raid:121	1	RAID Disk OK	/Monitor/RAID/DISK/Ok
raid:122	5	RAID Disk Rebuilding	/Monitor/RAID/DISK/Rebuilding
raid:123	8	RAID Disk Failed	/Monitor/RAID/DISK/Failed

Appendix B

Destination Runtime Parameters

The following table describes the destination parameters you can configure. The parameters listed in the table are not available for all destinations. The user interface automatically displays the parameters valid for a destination. For step-by-step instructions on updating the runtime parameters of a destination, see "Editing Connector Parameters" on page 74.

Name Fields	Value Fields
Batching	Connectors can batch events to increase performance and optimize network bandwidth. When activated, connectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires, whichever occurs first. You can also prioritize batches by severity, forcing the connector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, **100**, 200, 300 events).
Enable Batching (in seconds)	The connector sends the events if this time window expires (1, **5**, 10, 15, 30, 60).
Batch By	This is **Time Based** if the connector should send batches as they arrive (the default) or **Severity Based** if the connector should send batches based on severity (batches of Highest Severity events sent first).
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the connector to automatically correct the time reported by the device.
Use Connector Time as Device Time	Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. (**No** | Yes)
Enable Device Time Correction (in seconds)	The connector can adjust the time reported by the device `Detect Time`, using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol. The default is **0**.
Enable Connector Time Correction (in seconds)	The connector can also adjust the time reported by the connector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the connector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and connectors is the NTP protocol. The default is **0**.

Set Device Time Zone To	Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the connector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported. Default: **Disabled**.
Device Time Auto-correction	
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by `Past Threshold` seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by `Past Threshold` seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, `(ALL)`, means all devices.
Time Checking	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking. The default is **5 minutes** (300 seconds).
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is **1 hour** (3,600 seconds).
Frequency	The connector checks its future and past thresholds at intervals specified by this number of seconds. Default is **1 minute** (60 seconds).
Cache	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Cache Size	Connectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the connector receives bursts of events. This parameter specifies the disk space to use. The default is **1 GB** which, depending on the connector, can hold about 15 million events, but it also can go down to **5 MB**. When this disk space is full, the connector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 150 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is **10,000**.
Notification Frequency	How often to send notifications after the Notification Threshold is reached. (1 minute, 5 minutes, **10 minutes**, 30 minutes, 60 minutes.)
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the destination. The default is **10 seconds**, but it can go from **5 seconds** to **10 minutes**. Note that the heartbeat is also used to communicate with the connector; therefore, if its frequency is set to **10 minutes**, then it could take as much as 10 minutes to send any configuration information or commands back to the connector.
Enable Name Resolution	The connector tries to resolve IP addresses to hostnames, and hostnames to IP addresses, if required and if the event rate allows. This setting controls this functionality. The Source, Target and Device IP addresses and Hostnames might also be affected by this setting. By default, name resolution is enabled (**Yes**).

Name Resolution Host Name Only	Default: **Yes**.
Name Resolution Domain From E-mail	Default: **Yes**.
Clear Host Names Same as IP Addresses	Default: **Yes**.
Limit Bandwidth To	A list of bandwidth options you can use to constrain the connector's output over the network. (**Disabled**, 1 kbit/sec to 100 Mbits/sec.)
Transport Mode	You can configure the connector to cache to disk all the processed events it receives. This is equivalent to pausing the connector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (**Normal** | Cache | Cache (but send Very High severity events).
Address-based Zone Population Defaults Enabled	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping. Default: **Yes**.
Address-based Zone Population	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping.
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	Shows the URI of the zone associated with the connector's source address. (Required for ESM v3.0 compatibility.)
Source Translated Zone URI	Shows the URI of the zone associated with the connector's translated source address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Destination Zone URI	Shows the URI of the zone associated with the connector's destination address. (Required for ESM v3.0 compatibility.).
Destination Translated Zone URI	Shows the URI of the zone associated with the connector's translated destination address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Connector Zone URI	Shows the URI of the zone associated with the connector's address. (Required for ESM v3.0 compatibility.)
Connector Translated Zone URI	Shows the URI of the zone associated with the connector's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Device Zone URI	Shows the URI of the zone associated with the device's address. (Required for ESM v3.0 compatibility.)
Device Translated Zone URI	Shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)

Field Based Aggregation	This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, all the fields of the two events are the same (the only difference being the detect time). However, field-based aggregation implements a less strict aggregation mechanism; two events are aggregated if only the selected fields are the same for both alerts. It is important to note that field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored. Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate “accepts” and “rejects” in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (**Disabled**, 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (**Disabled**, 10 events, 50 events, and so on, up to 10,000 events.)
Field Names	Enter one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-hostnames. Names can contain no spaces and the first letter should not be capitalized.
Fields to Sum	Enter one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Preserve Common Fields	Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing **No**, the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events). Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (**Disabled**, 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (**Disabled**, 10 events, 50 events, and so on, up to 10,000 events.)

Fields to Sum	(Optional) Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Processing	
Preserve Raw Event	For some devices, a raw event can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field. This feature is disabled by default since using raw data increases the event size and therefore requires more database storage space. You can enable this by changing the **Preserve Raw Event** setting. The default is **No**. If you choose **Yes**, the serialized representation of the "Raw Event" is sent to the destination and preserved in the `Raw Event` field.
Turbo Mode	You can accelerate the transfer of a sensor's event information through connectors by choosing one of two “turbo” (narrower data bandwidth) modes. The default transfer mode is called **Complete**, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific). **Complete** mode does indeed use all the database performance advances of ArcSight ESM v3.x. The first level of Turbo acceleration is called **Faster** and drops just additional data, while retaining all other information. The **Fastest** mode eliminates all but a core set of event attributes, in order to achieve the best throughput. The specific event attributes that apply to these modes in your enterprise are defined in the self-documented `$ARCSIGHT_HOME/config/connector/agent.properties` file for the ArcSight Manager. Because these properties might have been adjusted for your needs, you should refer to this file for definitive lists. Only scanner connectors need to run in **Complete** mode, to capture the additional data. **Note**: Connector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to **Faster** will not pass all the data possible for a connector that is set for the default of **Complete**.

Enable Aggregation (in seconds)	When enabled, aggregates two or more events on the basis of the selected time value. (**Disabled**, 1, 2, 3, 4, 5, 10, 30, 60) The aggregation is performed on one or more matches for a fixed subset of fields: • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.
Limit Event Processing Rate	You can moderate the connector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts. The choices range from **Disabled** (no limitation on CPU demand) to **1 eps** (pass just one event per second, making the smallest demand on the CPU). Note: The effect of this option varies with the category of connector in use, as described in the connector Processing Categories table below.
Fields to Obfuscate	
Store Original Time in	**Disabled** or Flex Date 1.
Enable Port-Service Mapping	Default: **No**.
Enable User Name Splitting	Default: **No**.
Split File Name into Path and Name	Default: **No**.
Event Integrity Algorithm	**Disabled**, SHA-1, SHA-256, SHA-512, or MD5.
Generate Unparsed Events	Default: **No**.
Preserve System Health Events	Yes, **No**, or Disabled.

Enable Device Status Monitoring (in minutes)	**Disabled** or 1, 2, 3, 4, 5, 10, 30, 60, or 120 minutes.
Filters	
Filter Out	NA
“Very High Severity” Event Definition	NA
“High Severity” Event Definition	NA
“Medium Severity” Event Definition	NA
“Low Severity” Event Definition	NA
“Unknown Severity” Event Definition	NA
Payload Sampling	(When available.)
Max. Length	Discard, 128 bytes, **256 bytes**, 512 bytes, 1 kbyte
Mask Non-Printable Characters	Default: **False**.

Appendix C

Special Connector Configurations

Certain connectors require additional configuration when used with ArcSight Management Center. This appendix describes the additional configuration. For general information about installing connectors, see “Adding a Connector” on page 180.

The following topics are discussed here:

Microsoft Windows Event Log - Unified Connectors

The SmartConnector for Microsoft Windows Event Log - Unified is not part of a FIPS-compliant solution. When you add a Windows Event Log - Unified connector, be sure the container is not FIPS-enabled in order for the connector to collect events.

When adding a Windows Event Log - Unified connector, follow the specific instructions in the SmartConnector configuration guide for entering parameters, entering security certifications when using SSL, enabling audit policies, and setting up standard user accounts.

There are currently two parser versions for the Microsoft Windows Event Log - Unified SmartConnector.

- Parser Version 0 is generally available with each SmartConnector release
- Parser Version 1 is available with the Microsoft Windows Monitoring content

The Microsoft Windows Event Log - Unified SmartConnector configured for you during initial configuration uses Parser Version 1.

Detailed Security Event mappings for this parser version can be found in Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1 (MSWindowsEventLogUnifiedMappingsParserVersion1.pdf), available on HP ArcSight Protect724.

When you install additional Microsoft Windows Event Log Unified connectors, they are installed with the generally available base parser version (Parser Version 0). Mappings for

the base parser version are available with each SmartConnector release (Security Event Mappings: SmartConnectors for Microsoft Windows Event Log) and can be found on Protect 724, along with the SmartConnector configuration guide. You must use Parser Version 1 if you want the default Windows Monitoring content to work. For details see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified, or SmartConnector Configuration Guide for Microsoft Windows Security Events - Mappings.

The pre-bundled SmartConnector for Microsoft Windows Event Log - Unified installed using the First Boot Wizard is installed with Parser Version 1. Any Windows Event Log - Unified connectors you add using the connector configuration wizard are installed with Parser Version 0 (the base parser).

Change Parser Version by Updating Container Properties

A parser is a SmartConnector component that specifies how to parse the information contained in the device raw events, and how to map it to HP ArcSight security event schema fields. Parsers can be in the form of property files, map files, or CSV files. Each SmartConnector has its own parser or set of parsers.

Multiple parser versions lets each SmartConnector parse raw events in many different ways to generate ArcSight security events with appropriate mappings. The SmartConnector for Microsoft Windows Event Log -- Unified, supports two parser versions: Base Parser and Parser Version 1.

With multiple parser versions:

- One SmartConnector build supports multiple parser versions.
- Users can configure their connectors to use the available parser versions of their choice, depending on their event mapping requirements.
- Users can reconfigure connectors to use the appropriate parser version as needed.

Multiple parser versions currently are supported only for the SmartConnector for Microsoft Windows Event Log -- Unified. This functionality is not supported for user-developed ArcSight FlexConnectors.

Each SmartConnector has its own internal `fcp.version` parameter setting to represent its current parser version. The default value for the fcp.version parameter is the base (or default) parser version, which is Parser Version 0. Each SmartConnector can support a total of 8 parser versions. The `fcp.version` parameter values range from 0 through 7. Microsoft Windows Unified SmartConnector supports parser versions 0 and 1.

Be sure that when you have content with new mappings, you change the parser version to match that content.

To update container properties (located in the agent.properties file) to change the parser version being used when mapping events:

1. Click **Manage** from the top-level menu bar.
2. Select a navigation path.
3. Select the container whose properties you want to update. You can select multiple containers.
4. Click **Properties**.
5. Follow the instructions in the wizard to update connector properties.

The `fcp.version` parameter value 0 designates the base parser. To use parser 1, change the `fcp.version` parameter value to 1. For example:

```
agents[0].fcp.version=1
```

SSL Authentication

If you choose to use SSL as the connection protocol, you must add security certificates for both the Windows Domain Controller Service and for the Active Directory Server. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic. With the First Boot Wizard installation of the connector, the certificates are already imported for you. If you add Windows Event Log - Unified connectors, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for instructions.

Database Connectors

The following database connectors are available for installation with ArcSight Express:

- IBM SiteProtector DB*
- McAfee ePolicy Orchestrator DB*
- McAfee Vulnerability Manager DB*
- McAfee Network Security Manager DB*
- Microsoft SQL Server Audit Multiple Instance DB*
- Oracle Audit DB
- Symantec Endpoint Protection DB*
- Trend Micro Control Manager NG DB*
- Snort DB*

*These connectors extract events from an SQL Server or MySQL databases, which requires a JDBC driver. See “Add a JDBC Driver” on page 188 for instructions.

All of these database connectors require the following information when being added to ArcSight Express; some connectors require additional parameters, such as event types or polling frequency.

Parameter	Description
Database JDBC Driver	If you are using an ODBC DRIVER, select 'sun.jdbc.odbc.JdbcOdbcDriver' driver. For JDBC drivers, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver. If you are using an ODBC DRIVER, select 'sun.jdbc.odbc.JdbcOdbcDriver' driver. For JDBC drivers, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.

Parameter	Description
Database URL	If you are using an ODBC DRIVER, enter: 'jdbc:odbc:<ODBC Data Source Name>, where the <ODBC Data Source Name> is the name of the ODBC data source you just created. If you are using a JDBC DRIVER, enter: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>,' substituting actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.
Database User	Enter the login name of the database user with appropriate privilege.
Database Password	Enter the password for the SiteProtector Database User.

Add a JDBC Driver

The IBM SiteProtector DB, McAfee ePolicy Orchestrator DB, McAfee Vulnerability Manager DB, McAfee Network Security Manager DB, Microsoft SQL Server Audit Multiple Instance DB, Symantec Endpoint Protection DB, and Trend Micro Control Manager NG DB connectors extract events from a SQL Server database. For information about and to download the MS SQL Server JDBC Driver, see:

http://msdn.microsoft.com/en-us/sqlserver/aa937724

Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

The SmartConnector for Snort DB extracts events from a MySQL database. For information about and to download the MySQL JDBC Driver, see:

http://dev.mysql.com/downloads/connector/j/5.0.html

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as follows:

1. From ArcSight Express, select **Setup -> Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, and then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the *.jar* file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all files you require, click **Next**.

9 In the **Name** field, enter a descriptive name for the zip file (`JDBCdriver`, for example). Click **Next**.

10 Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.

11 To apply the driver file, select the driver `.zip` file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.

12 Select the container or containers into which the driver is to be uploaded; click **Next**.

13 Click **Done** to complete the process.

Configuration guides for the database connectors supported with ArcSight Express can be found on the Protect 724 community. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Protect 724:

- IBM SiteProtector DB
- McAfee ePolicy Orchestrator DB
- McAfee Vulnerability Manager DB (formerly FoundScan)
- McAfee Network Security Manager DB
- Microsoft SQL Server Multiple Instance Audit DB
- Oracle Audit DB
- Symantec Endpoint Protection DB
- Trend Micro Control Manager DB
- Snort DB

API Connectors

The following API connectors are available for installation with ArcSight Express. They require a client and authentication credentials, as well as configuring the events types to be sent to the connector by the device.

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

For Cisco Secure IPS SDEE, if you want the SmartConnector to validate the Cisco IPS sensor's authentication certificate, obtain the authentication certificate from the IPS sensor and import it to the appliance.

For Sourcefire Defense Center eStreamer, add an eStreamer client, create an authentication certificate, and select event types to be sent to the connector.

See the individual configuration guides for these connectors for instructions.

Follow the instructions in "Uploading Certificates to the Repository" in the Connector Management for ArcSight Express 4.0 User's Guide to import the trusted certificates to ArcSight Express.

Configuration guides for the API connectors supported with ArcSight Express can be found on the Protect 724 community. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Protect 724:

- Cisco Secure IPS SDEE

- Sourcefire Defense Center eStreamer

File Connectors

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS).

The following File connector is available for installation with ArcSight Express:

- Blue Coat Proxy SG Multiple Server File

See the configuration guide for device setup, parameter configuration, and mappings information for the SmartConnector for Blue Coat Proxy SG Multiple Server File.

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS). For the file-based connectors on a Windows system, configure a CIFS share before you add the connectors.

For information on creating a CIFS Mount or an NFS Mount, see "Managing a Remote File System" in the Connector Management for ArcSight Express 4.0 User's Guide.

Syslog Connectors

If you selected Syslog Daemon during initial installation with the First Boot Wizard, the Syslog Daemon connector has already been installed.

You can add a Syslog File, Pipe, or Daemon connector in a new container. Syslog connectors for the following devices are available with ArcSight Express:

- Cisco PIX/ASA Syslog
- Cisco IOS Router Syslog
- Juniper Network and Security Manager Syslog
- Juniper JUNOS Syslog
- UNIX OS Syslog

Be sure your device is set up to send syslog events. See your device documentation or the SmartConnector Configuration Guide for device configuration information; the guide also includes specific device mappings to ArcSight event fields as well as further information needed for configuration if you are installing the Pipe or File connectors. Mappings in the SmartConnector for UNIX OS Syslog configuration guide apply to all syslog connectors. Specific mappings per device are documented in the configuration guide for the device.

Configuration guides for these syslog connectors supported with ArcSight Express can be found on the Protect 724 community:

- Cisco PIX/ASA Syslog
- Cisco IOS Syslog
- Juniper JUNOS Syslog
- Juniper Network and Security Manager Syslog
- UNIX OS Syslog

Index

Symbols

A

B

C

D

E

F

H

I

L

M

N

P

R

S

T

U