Administrator's Guide

ArcSight™ Connector Appliance v6.2

September 13, 2011

ArcSight™
An HP Company

Administrator's Guide
ArcSight™ Connector Appliance v6.2

Revision History

Date	Product Version	Description
09/13/2011	6.2	GA release with new features: New permission options for User Groups, read-only default option, automatic password reset, forgot password option, ability to download multiple destination certificates, FTP for BlueCoat SmartConnector, custom login banner, new audit events, NTLMv2 authentication, LDAP/AD, and SNMPv2.
05/09/2011	6.1	GA release with new features: Diagnostics on a Container, Developing FlexConnectors (including new appendix on Regular Expressions), new options for Backup and Restore, About menu item, and new Troubleshooting and FAQ appendix.
02/05/2011	6.1 Beta	Added configuration information for event forwarding. Added new feature documentation: Diagnostics on a Container, Developing FlexConnectors (including new appendix on Regular Expressions), and Save to Local option for Backup and Restore.
09/17/2010	6.0 GA	Added system health event descriptions.
08/01/2010	6.0 Beta	Added new features.

Document template version: 1.0.2.9

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal
Protect 724 Community	https://protect724.arcsight.com

Contents

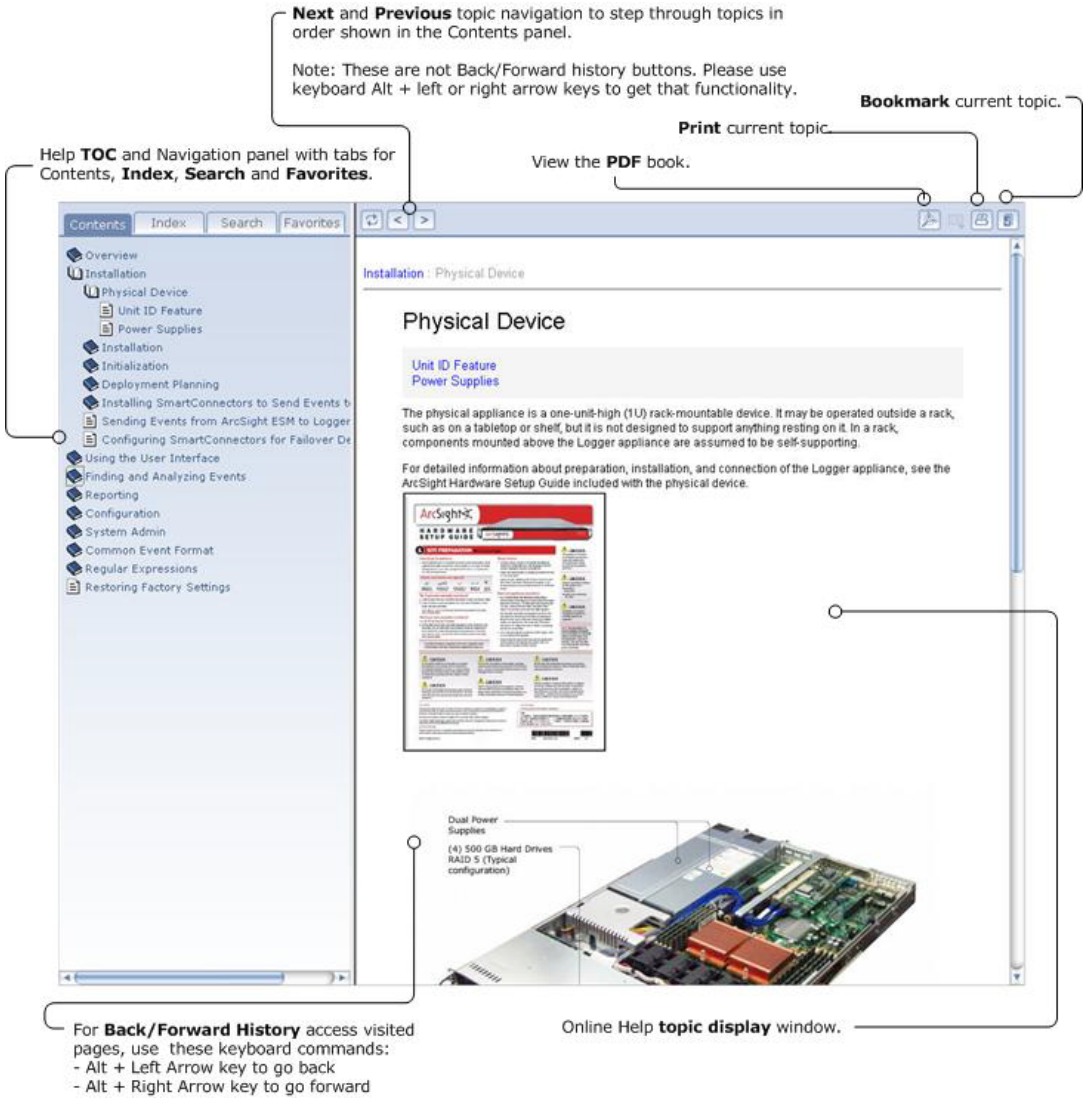
About this Guide

The ArcSight Connector Appliance Administrator's Guide describes how to install, configure, and use your Connector Appliance.

The following topics are discussed here.

About the Online Help

Online Help for the Connector Appliance is delivered in both Web-based (HTML) and PDF formats. To access the Online Help, click **Help** on the Connector Appliance GUI. The Web-based Help is context-sensitive; choosing Help displays the topic(s) related to the currently displayed user interface page.



The Online Help includes the following features.

- Left panel Help navigation - Click a tab for **Contents (TOC)**, **Index**, **Search**, or **Favorites**.

  The TOC tracks with your navigation of the Help topics in the main display. The Index provides alphabetical “jump to” points. You can bookmark frequently referenced topics as “Favorites.”

- **Next**, and **Previous** sequential topic navigation to step through topics in order shown in the Contents (TOC) panel. Click the Previous button ( ) to view the preceding topic in the history, or the Next button ( ) to view the subsequent topic.

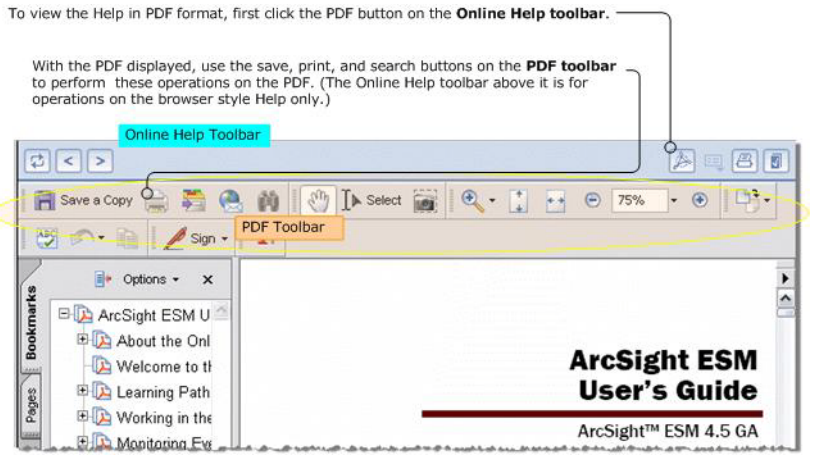
> **Tip**
>
> For **Back/Forward History** access to visited pages (like Back/Forward buttons on a Web browser), use these keyboard commands:
>
> - **Alt + Left Arrow key** to go **Back**
> - **Alt + Right Arrow key** to go **Forward**

- Topic display window - Click a topic in the Contents, Index, Search hit list, or saved Favorites to view it in the display window.
- Breadcrumbs - The top of each HTML page on the main Help display shows your location in the topic list. Click on the “parent topic” to return to it. (The left panel TOC also tracks your location within the topics.)
- Access to the Help as an Adobe Acrobat PDF document.

  Click the **PDF** button ( ) in the upper right of the Online Help toolbar to open the PDF. The Help is displayed as a print-friendly PDF within the Help window. All Adobe Acrobat PDF features (Bookmarks TOC, Hyperlinks, Search, Zoom, Comments, Print, Sign, E-mail, and so on) are available on the PDF from within the Console Help window.

  To view the PDF outside of the Help display, click the **Save** button to **download a copy of the PDF** to a selected location. Use the browser to navigate to the directory where you want to save the file, and click **Save**.

  To **print the PDF**, click the Print button on the PDF toolbar.



- Print capabilities - Click the **Print** button to print a copy of the **current topic**.

  To **print the PDF**, first click the **PDF** button in the upper right of the main Web Online Help toolbar to get PDF click, then click the **Print** button on the **PDF toolbar**.

- Bookmarks - Click the Bookmark ( ) button and follow the instructions in the popup window to bookmark a topic.

Who Should Read this Guide

This guide is intended for Connector Appliance administrators and users. You should have a good understanding of SmartConnectors, ArcSight ESM, and/or ArcSight Logger.

Related Documentation

The latest and most complete set of documentation for the ArcSight Connector Appliance is always offered on the ArcSight Customer Support site (http://www.arcsight.com/supportportal) through the Product Documentation link in the Knowledge Center section.

Feedback

To submit feedback about the ArcSight Connector Appliance or the ArcSight Connector Appliance documentation, visit the ArcSight Customer Support web site at http://www.arcsight.com/supportportal.

Chapter 1

Introducing the Connector Appliance

The following topics are discussed here.

Connector Appliance Overview

ArcSight Connector Appliance is a hardware solution that incorporates a number of onboard ArcSight connectors (also known as SmartConnectors) and a web-based user interface that provides centralized management for connectors across a number of hosts.

Connectors are ArcSight software components that forward *events* from a wide variety of devices and security event sources to ArcSight Logger or ArcSight ESM.

The Connector Appliance centralizes connector management and offers unified control of connectors available on:

- The local Connector Appliance
- Other Connector Appliances
- Software-based connectors (running on any network-accessible host, such as Windows or UNIX)

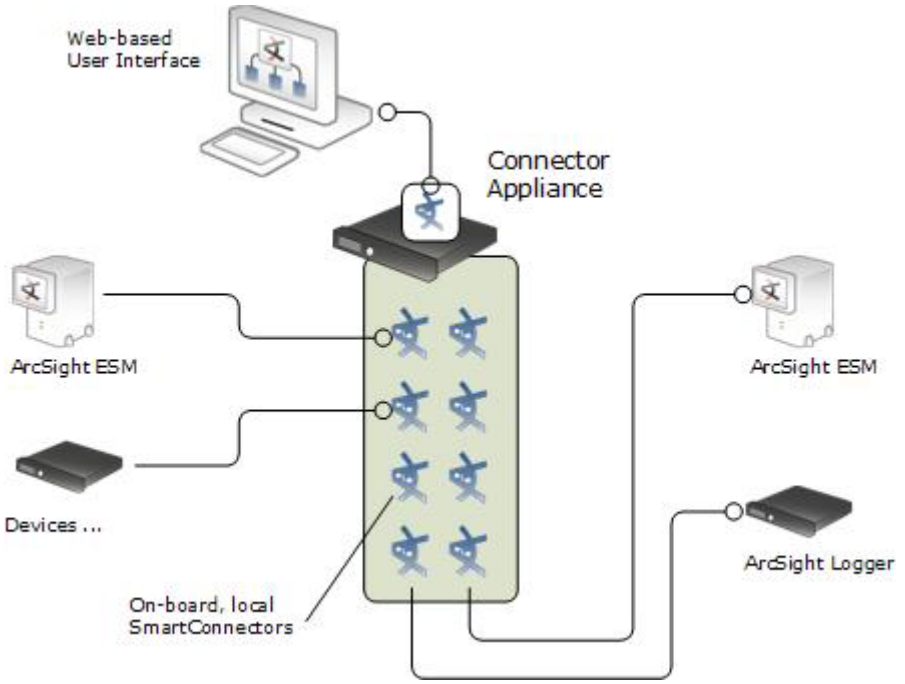


Figure 1-1 ArcSight Connector Appliance Deployment

The Connector Appliance delivers the following features and benefits.

- Supports bulk operations across all connectors and is particularly desirable in ArcSight ESM and ArcSight Logger deployments with a large number of connectors, such as a Managed Security Services Provider (MSSP).
- Provides an ArcSight ESM-like connector management facility in Logger-only environments.
- Provides a single interface through which to configure, monitor, tune, and update connectors. Because the Connector Appliance does not receive events from the connectors it manages, it can manage many of them at one time. The Connector Appliance does not affect working connectors unless it is used to change their configuration. In such cases, the connector is commanded to restart.

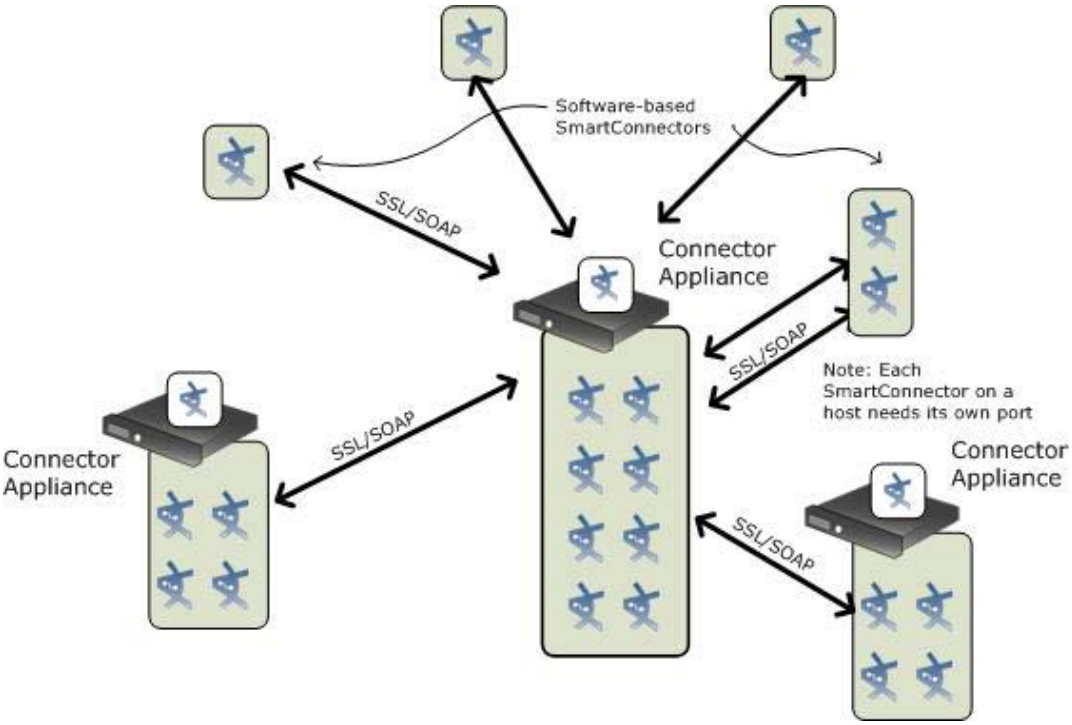


Figure 1-2 Connector Appliance Manages All Your Connectors

Connectors that forward events to ArcSight ESM can be managed using the ESM Console; the Connector Appliance is not required if all connectors have ESM as their only destination. However, the Connector Appliance is useful when connectors target multiple heterogeneous destinations (for example, when ArcSight Logger is deployed together with ESM), in a Logger-only environment, or when a large number of connectors are used, such as in a MSSP deployment.

Connector Appliance connectors operate within *containers*. Each container runs its own Java Virtual Machine (JVM). Containers contain one or more connectors. There can be multiple containers on a Connector Appliance.

Connectors

Connectors read Events from devices, parse and normalize them, then forward them to various destinations.

The Connector Appliance manages three types of connectors:

- Local (on-board) connectors
- Remote Connector Appliance connectors
- Remote software-based connectors (running on any network-accessible host, such as Windows and UNIX)

Local (On-Board) Connectors

The Connector Appliance includes multiple containers and on-board connectors. You can use the appliance interface to manage these local connectors as well as remote connectors.

High load on the on-board connectors might impact performance of the Connector Appliance web-based interface.

Remote Connector Appliance Connectors

The Connector Appliance can manage connectors on remote Connector Appliances, as well as other ArcSight hardware solutions such as ArcSight Logger (only on models that support onboard connectors).

Software-Based Connectors

The Connector Appliance can remotely manage connectors running on any network-accessible host. These connectors need to be configured for remote management.

- Only fifth-generation connectors support remote management. To use this feature, you need connector **build 4855 (4.0.5.4878.0)** or later.
- If you install software connectors on your own hardware, you need to add the parameters `remote.management.enabled=true` and `remote.management.listener.port=`*`port_number`* in the `agent.properties` file. Refer to "How do you manage software connectors on remote hosts?" on page 210.
- Connector Appliance cannot remotely manage connectors running on AIX.

Multiple software-based connectors installed on the same host require a separate port assignment. The default port for ArcSight connectors is **9001**. A second connector installed on the same host needs to use an alternate port. ArcSight recommends using port 9002, 9003, 9004, and so on.

Supported Connectors

For a complete list of all connectors supported by the Connector Appliance, visit the ArcSight Customer Support web site at http://www.arcsight.com/supportportal. ArcSight adds new connectors regularly.

Events

An event is a record of activity that takes place on a network, OS, application, physical security system, or database. ArcSight connectors are the vehicle by which events travel to their destination(s), which might include ArcSight ESM, ArcSight Logger, a syslog or log file.

Event Source Types

Within an ArcSight deployed network, a *device* is defined as hardware or software capable of logging or outputting security events—that is, acting as a source of events. Devices such as intrusion detection and prevention systems, operating systems, routers and other network equipment, vulnerability scanners, web servers, and other security software are all sources for events. They are sent in formats such as *syslog*, *log files*, and *databases*.

ArcSight ESM itself can be considered a device (or source of events) using the ArcSight Forwarding connector.

Event Processing

The event processing performed by ArcSight connectors includes normalization, optional time correction, filtering, and aggregation. *Normalization* describes all security events using the same format so that events from multiple sources can be compared and correlated meaningfully. *Time correction* allows you to correct the time reported by the device automatically. *Filtering* and *aggregation* significantly decrease the amount of data received and increase data relevancy.

Event Destinations

Event destinations include ArcSight ESM (or ArcSight Manager), ArcSight Logger, CEF syslog, or a log file.

Manager

When connectors send events to an ArcSight ESM Manager, the Manager stores the events in a relational database, processes them using its correlation engine, and makes them visible to the ArcSight Console or ArcSight Web interfaces.

Logger

Connectors can send CEF events to ArcSight Logger using an encrypted, optionally compressed, channel called SmartMessage. Logger can also receive CEF Syslog events from connectors.

CEF Syslog

Connectors can forward events as syslog messages. In this case, the normalized event is sent using Common Event Format (CEF) which uses name/value pairs. The Connector Appliance can send syslog over UDP or TCP.

Failover Destination

Each connector destination can have a failover destination. When communication with the primary destination fails, the connector automatically begins sending events to the designated failover destination. Failover only works with communication protocols that can detect transmission failure, such as TCP. For steps on creating a failover destination, see "Adding a Failover Destination to a Specific Connector" on page 141.

Alternate Configurations

You can define alternate configurations for connectors and specify when the alternate is to be active. For example, a different destination or failover destination can be specified for weekends or for early morning hours.

Other connector properties might change at certain times. For example, to reduce the number of events moving on the network, aggregation might be specified during peak times.

For the steps to edit an alternative configuration, see "Editing an Alternate Configuration" on page 150.

Deployment Scenarios

You can deploy the Connector Appliance wherever ArcSight connectors are needed. Connector Appliance provides the following benefits.

- Connector management without ArcSight ESM (that is, Logger-only environments).
- Remote control of runtime parameters, such as bandwidth control.
- Centralized connector upgrade management and control.
- Central troubleshooting of specific connectors.

ArcSight ESM

Deploying the Connector Appliance in an ArcSight ESM environment centralizes connector upgrade, log management, and other configuration procedures. For more information, see Chapter 4, Backup and Restore, on page 27.

ArcSight Logger

ArcSight Logger receives and sends events from and to ArcSight connectors, but lacks the depth of connector management found in ArcSight ESM.

A Logger-only deployment benefits from the Connector Appliance in many capacities, and provides most of ESM's management functionality, but not all (for example, it does not contain the filter designer). The Connector Appliance also offers new features, such as bulk operations (enabling control of many connectors at one time), that ESM does not.

Connector Appliance can also configure connectors with failover destinations, providing central failover control when redundant Loggers are deployed for this purpose. All or some connectors can be configured to send events to a second Logger, or to an event file in the case of communication failure with the primary destination.

ArcSight ESM and Logger

Connector Appliance centralizes control when events are sent to ESM and Logger simultaneously. In one scenario, all events are sent to Logger while only high-value events are sent to ESM (for further analysis). In another scenario, all events are sent to both, but Logger implements a longer retention policy.

Although each connector has specific destination parameters, the Connector Appliance allows for "bulk" management, removing the need to manually access each remote connector host to add or change destinations.

Chapter 2

Installing the Connector Appliance

The following topics are discussed here.

Installation Requirements

Although there are no special requirements for installing the Connector Appliance on your network, confirm that you have a computer with a standard browser, such as **Mozilla Firefox** or **Microsoft Internet Explorer**. The computer should be in close proximity to the network rack where you install the appliance or a serial port, or a monitor and keyboard.

For specific browser versions, refer to the most recent Connector Appliance Release Notes.

Unpacking and Installing your Connector Appliance

To unpack, install, and connect to your appliance for the first time, follow the instructions in the *Getting Started with ArcSight Connector Appliance* document that ships with your appliance.

Although the *Getting Started with ArcSight Connector Appliance* document is included in printed form with the appliance, you can download it in PDF format from the ArcSight Customer Support site at `http://www.arcsight.com/supportportal`.

Connecting for the First Time

The Connector Appliance ships with these default IP addresses:

- On Eth0: 192.168.35.35 (subnet mask 255.255.255.0)
- On Eth1: 192.168.36.35 (subnet mask 255.255.255.0)
- On Eth2: 192.168.37.35 (subnet mask 255.255.255.0)

The number of network connectors varies based on the hardware platform.

Installing a License

Connector Appliance requires a valid license file to enable the management features. You need to install a valid license on your Connector Appliance before proceeding further. For information about obtaining and installing a license, contact ArcSight Customer Support.

Upgrading

For version specific information on upgrading from one version of Connector Appliance to another, refer to the most recent Connector Appliance Release Notes.

Configuring Platform Settings and Objects

After you have installed a license on your appliance, you can use the **Connector Appliance Deployment Wizard** to configure additional platform settings, connectors, and remote hosts that you want to manage. The wizard offers a simple and intuitive interface that enables you to perform these configurations quickly.

The deployment wizard displays automatically when you first connect to Connector Appliance and after you have installed a license. Follow the prompts to configure the platform settings and objects (connectors and remote hosts) you want to manage. The deployment wizard offers two levels of setup:

- **Express** offers a quick start to basic configuration. It provides a limited, but most typical set of minimal parameters. This setup level is appropriate for environments that require Syslog or Windows connectors, and a Logger-only destination.
- **Advanced** offers full control of connector and destination setup, including remote management and configuration steps for all available connector types.

Depending on which setup option you choose, follow the prompts to add remotely-managed connectors and remote hosts. When complete, the wizard confirms your changes and prompts you to reboot for the changes to take effect.

Changing the Default Password

After initial set up is complete, ArcSight strongly recommends that you change the default password to a secure password. To update the password, follow the instructions in “Change Password” on page 65.

Chapter 3

Understanding the User Interface

The following topics are discussed here.

Overview

The Connector Appliance uses a web-based user interface and requires **Mozilla Firefox 3.6** or **6.0**, or **Microsoft Internet Explorer 8.0** or **9.0**. A Flash plug-in is also required. Adobe Acrobat reader software is required to read this document in PDF format.

This chapter provides a general overview of the Connector Appliance interface. The following chapters of this guide describe the primary tabs in detail.

- The **Monitor** tab is described in "Monitoring the Connector Appliance" on page 169.
- The **Manage** tab is described in "Managing Connectors" on page 97.
- The **Setup** tab is described in "Backup and Restore" on page 27 and Chapter 6, Managing Repositories, on page 71.

Each component of the Connector Appliance user interface uses one or all of these navigational and functional elements:

- Main page links
- Function tabs
- A left panel menu of options, submenus, and commands
- Component-based action buttons and links

Main Page Links

Most of these elements are shown independently of the component you are currently using, and provide navigational access and online help throughout your use of Connector Appliance.

The ArcSight logo in the upper-left corner of the user interface is one of the first elements of the Connector Appliance main page. Hover over this logo to verify your Connector Appliance version number.

Gauges at the top of the screen provide an indication of throughput and CPU usage (with additional details under the Monitor tab). The name of the currently logged-in user is shown below the statistics.

The Options section (described below) explains how to change the default range of the gauges.

Help

Click **Help** to display the online help in a separate browser window.

About

Click **About** to display information about the Connector Appliance, such as the version number, and the copyright and trademark details.

Options

Click **Options** to set the range on the EPS In and EPS Out gauges. If the event rate exceeds the specified maximum, the range is increased automatically.

Logout

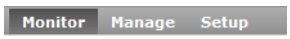
Click **Logout** to end your Connector Appliance session. ArcSight recommends that you log out before you leave the Console unattended.

Unless you are displaying the Monitor page, the system times out after a certain period of inactivity and logs you out automatically. The Monitor page, however, maintains a continuous session to allow for dashboard-style monitoring.

The Monitor page remains vulnerable when unattended. Use caution when stepping away during a Monitor-page session.

Function Tabs

The function tabs represent the main components of Connector Appliance.



- The **Monitor** tab displays graphs of recent and current system performance. The Monitor tab contains three sub-tabs:
  - Summary shows CPU usage and event flow on 4-hour, daily, and weekly scales.
  - Platform shows CPU usage, platform memory usage, receive, transmit, disk read, and disk write values for selectable time periods: 4 hours, daily, or weekly.
  - Network 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 for selectable time periods: 4 hour, daily, or weekly.

  See Chapter 8, Monitoring the Connector Appliance, on page 169.
- The **Manage** tab is the heart of the Connector Appliance interface. From this tab, you can configure connectors, send commands, and manage remote hosts. See Chapter 7, Managing Connectors, on page 97.
- The **Setup** tab enables you to configure your Connector Appliance, backup and restore the Connector Appliance configuration, and manage repositories that store

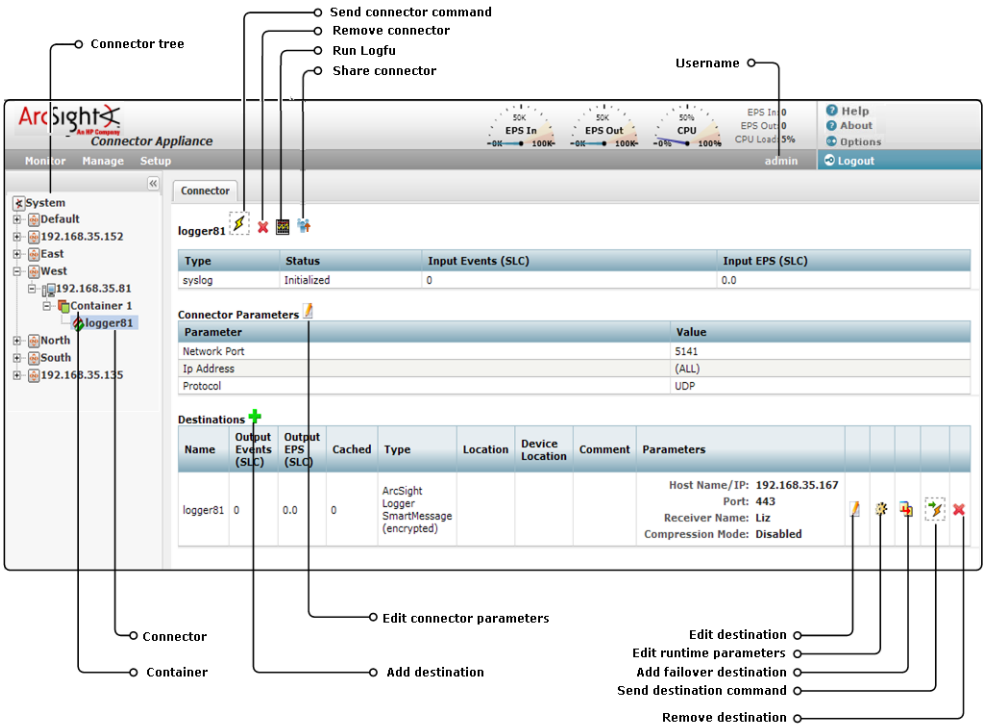
files, certificates, and drivers. See Chapter 4, Backup and Restore, on page 27 and Chapter 6, Managing Repositories, on page 71.

Menu Panel

The menu of commands on the left panel depend on the function tab you select. If you select the Manage tab, only the functions used when managing connectors are displayed. For details about the menu panel of each function tab, see the appropriate chapter in this guide.

Component-Based Action Buttons and Links

These elements are linked to specific tasks you can perform on the currently-displayed user interface page, as shown in the example below.



For details about the action buttons and links of each component, see the appropriate chapter in this guide.

Chapter 4

System Admin - Connector Appliance

This chapter describes the System Admin tab that enables you to configure network, storage, and security settings for your system. Additionally, you can create and manage users and user groups using this tab.

The following topics are covered in this chapter:

System

From the System tab, you can configure system specific settings such as network settings (if applicable) and SMTP.

Reboot

To reboot your ArcSight System:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Reboot** from the System section.
3. Click **Start Reboot Now**.

   Your system will reboot in about 60 seconds. The boot process normally takes 5-10 minutes, during which time the system is unavailable.

Network

You can configure the DNS, Hosts, NICs, static routes, and system time settings under the Network menu.

System DNS

To change DNS settings:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** from the System section.
3. In the **System DNS** tab, enter new values for the IP address of the primary and secondary DNS servers, or edit the list of search domains.

   To add a new domain, click the  icon. To remove a domain, click the  icon. To change the search order of domains, select a domain name and click the up or down arrows until desired order is established.
4. Click **Save** to save the changes. Then, click **Restart Network Service** for changes to become effective.

Hosts

The Hosts tab allows direct editing of your system's /etc/hosts.txt file. You can enter data in the System Hosts text box or import it from a local file.

To change the Hosts information:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** from the System section.
3. In the Hosts tab, enter hosts information—one host per line—in the System Hosts text box in this format:

   <IP Address> <hostname1> <hostname2> <hostname3>

   If you want to import information from a file, click **Import from Local File** and locate the text file on the computer from which you are accessing your ArcSight system.
4. Click **Save** to save the changes. Then, click **Restart Network Service** for changes to become effective.

NICs

The NICs tab enables you to set the IP addresses for the network interface cards (NICs) on your system. Additionally, you can configure the hostname and default gateway for your system.

To set or change the NICs settings:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Network** from the System section.

3 In the **NICs** tab, enter these settings. To edit the IP address, subnet mask, or speed/duplex of a NIC, select the NIC and click **Edit** above the NIC Name list.

Setting	Description
Default Gateway	The IP address of the default gateway.
Hostname	The network host name for this system. Make sure that your DNS can resolve the host name you specify to your system's IP address. Performance is significantly affected if DNS cannot resolve the host name. This name must be identical to the domain specified in the Certificate Signing Request, described in "Generating a Certificate Signing Request" on page 50. **Note:** If you use a CA-signed certificate on this system and you are changing its host name, you must generate a new CSR, obtain a new certificate for your system, and upload it to ensure that the connectors (in FIPS mode) that communicate with your system will be able to validate the host name. For more information about generating a CSR, see "Generating a Certificate Signing Request" on page 50.
Automatically route outbound packets (interface homing)	When this feature is enabled (checked box), the response packets are sent back on the same system interface on which the request packets had arrived. Doing so can improve performance as the routing decisions do not need to be made (using the default gateway information and static routes) to send packets out from your system. If you have default gateway and static routes configured, they are ignored when this feature is enabled. When this feature is disabled (unchecked box), the default gateway and static routes (if configured) are used to determine the interface through which the response packets should leave your system. If you configure only one network interface, this setting does not provide any additional benefit.
IP Address	The IP address for each network interface card (NICs) in your system.
Subnet Mask	The subnet mask associated with the IP address you entered for a NIC.

Setting	Description
Speed/Duplex	Choose a speed and duplex mode, or let your system automatically determine the network speed: Auto (recommended) 10 Mbps - Half Duplex 10 Mbps - Full Duplex 100 Mbps - Half Duplex 100 Mbps - Full Duplex 1 Gbps - Full Duplex

4 Click **Save** to save the changes. Then, click **Restart Network Service** for changes to become effective.

Static Routes

You can specify static routes for the NICs on your system.

To add a static route:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Network** from the System section.

3 In the **Static Routes** tab, click **Add** to add a new static route. To edit or delete an existing route, select the route first, then click **Edit** or **Delete**.

When adding or editing a static route, you need to configure these settings.

Setting	Description
NIC	The network interface card (NIC) to which the static route applies
Type	Whether the static route is to a Network or a Host
Destination	The IP address for the static route destination
Subnet Mask	The subnet mask if you specify a network as the destination
Gateway	The IP address for the default gateway

4 Click **Save** to save the changes.

Time/NTP

The Time/NTP tab enables you to configure system time, date, local timezone, and NTP servers. ArcSight strongly recommends using an NTP server instead of manually configuring time and date on your system.

To set or change the system time, date, or timezone **manually**:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Network** from the System section.

3 In the **Time/NTP** tab, configure these settings.

Setting	Description
Current Time Zone	The time zone appropriate to your system's location.
Current Time	The current date and time at the system's location. To change this setting, click **Change Date/Time...**

The Time Zone change requires you to reboot the appliance. However, the Current Time change takes affect immediately.

To configure your system as an NTP server or for using an NTP server for your system:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Network** from the System section.

3 Click the **Time/NTP** tab.

4 Under **NTP Servers**, configure these settings.

To add a new NTP server, click the  icon. To remove a server, click the  icon.

To change the order in which the NTP servers should be used, select a server and click the up or down arrow until desired order is established.

Setting	Description
Enable as an NTP server	Check this setting if this system should be used as an NTP server.
NTP Servers	Enter the host name of an NTP server. For example, time.nist.gov. ArcSight recommends using at least three NTP servers to ensure precise time on your system. To enter multiple NTP servers, type one server name per line. Once you add servers to this list, you can click the "Click to Test" link to verify if the servers you added are reachable from your system. Notes: • An ArcSight system can serve as an NTP server for any other ArcSight system. • If System A serves as an NTP server for System B, System B needs to list System A in its NTP Servers list. • Use the **Test Servers** button to verify the status of the servers entered into the **NTP Servers** box.

You may need to scroll down to view the **Save** button and **Restart NTP Service**.

5 Click **Save** to save the changes. Then, click **Restart NTP Service** for changes to become effective.

SMTP

Your system uses the Simple Mail Transfer Protocol (SMTP) setting to send email notifications such as alerts, password reset emails, and so on.

To set or change SMTP settings:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **SMTP** from the System section and enter these settings.
3. Click **Save** to save the changes.

License & Update

You can update your appliance's software or apply a license to it on this page. This page also displays the elapsed time since the appliance was last rebooted, license information, and the version of the appliance components.

Updating the appliance software requires uploading an upgrade file you downloaded from the ArcSight Customer Support web site.

To update an appliance:

1. Download the update file from the ArcSight Download Center at https://arcsight.subscribenet.com to the computer from which you are accessing the appliance's user interface.
2. Connect to the appliance's user interface.
3. Click **Setup > System Admin** from the top-level menu bar.
4. Click **License & Update** from the System section.
5. Click **Browse** to locate the file.
6. Click **Upload Update**.

System Update will take effect after the next reboot. To update immediately, reboot the system after performing a System Update. See "Reboot" on page 28. A reboot is not required if you are only updating the license.

To apply a license file to an appliance:

1. Download the update file from the ArcSight Download Center at https://arcsight.subscribenet.com to the computer from which you can connect to the appliance.
2. From the computer to which you downloaded the update file, log in to the appliance's user interface using an account with administrator (upgrade) privileges.
3. Click **Setup > System Admin** from the top-level menu bar.
4. Click **License & Update** from the System section.
5. Browse to the *license* file you downloaded earlier and click **Upload Update**.

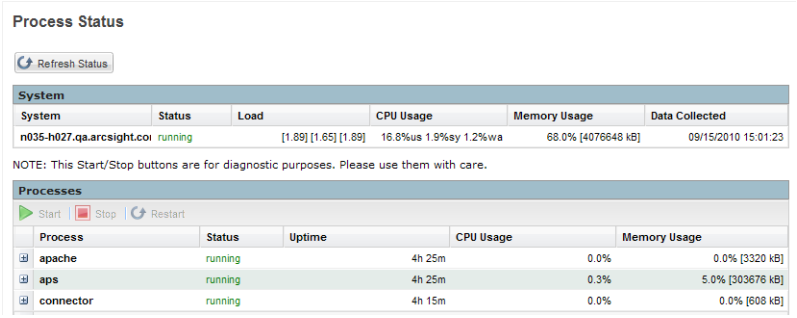
   Wait until a the user interface displays a message indicating that the upload was successful. You do not need to reboot your system after applying a license file.

Process Status

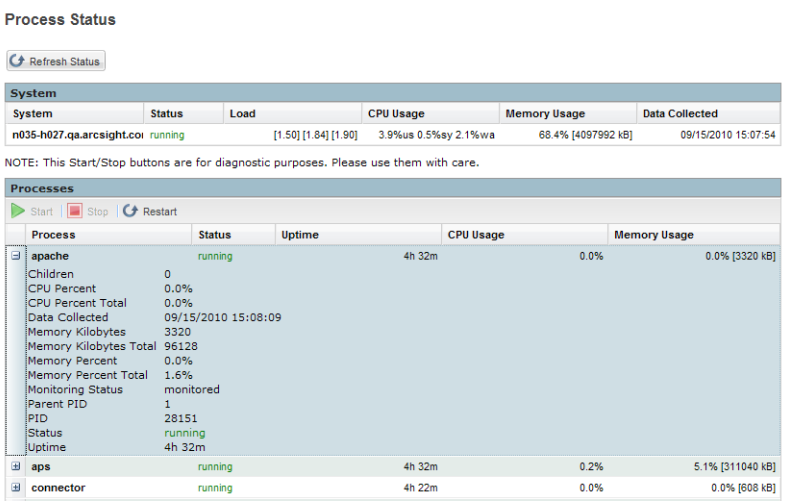
The Process Status page lists all processes related to your ArcSight system and enables you to view the details of those processes and start, stop, or restart them.

To view the Process Status page:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Process Status** from the System section to display a page similar to the one shown in the following figure.



To view the details of a process, click the icon to the left of the process name, as shown in the following figure.



To start, stop, or restart a process, select the process and click **Start**, **Stop**, or **Restart** at the top of the process list.

SSH Access to the Appliance

When you report an issue to ArcSight Customer Support that requires them to access your appliance for troubleshooting and diagnostics in situations such as an upgrade failure, unresponsive appliance, and so on, they will direct you to enable SSH access on it.

By default, SSH access (known as Support Login in previous releases) to your appliance is disabled; however, you can select one of these options in the appliance's user interface to enable it:

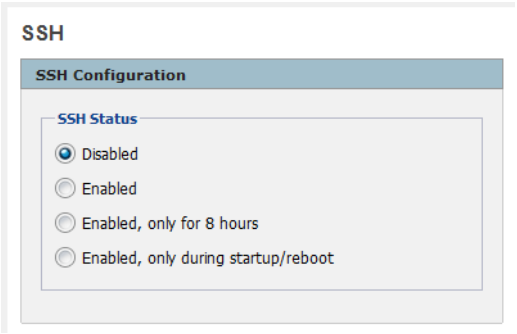
- Enabled—SSH access is always enabled.
- Enabled, only for 8 hours—SSH access is automatically disabled eight hours after it was enabled.
- Enabled, only during startup/reboot—SSH access is enabled during the time the appliance reboots and is starting up. It is disabled once all processes on the appliance are up and running. This option provides a minimal period of SSH access for situations such as when the appliance does not start successfully after a reboot.

Even if SSH is disabled on your appliance, you can access its console if you have it setup for remote access using the HP ProLiant Integrated Lights-Out (iLO) Advanced remote management card.

Enabling or Disabling SSH Access

To enable or disable SSH access to your appliance:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **SSH** from the System section.
3. Select one of the following options.



Once you select an option, the user interface displays a message that requires you to confirm the action. Once you confirm it, the change takes effect.

Connecting to Your Appliance Using SSH

Once you have enabled the SSH access, follow these steps to connect to it using SSH:

1. Connect to the appliance as "root" using an SSH client.
2. When prompted to enter a password, enter any text and press **Enter**.

   You are prompted to enter a response to the challenge string that is displayed on your screen.

3 Call ArcSight Customer Support to obtain the challenge response string. Enter it at the "Enter response:" prompt and press **Enter**.

```
login as: root
root@192.168.36.29's password:
Last login: Thu Mar 17 01:50:38 2011 from 10.4.10.190
Challenge is 46024. Enter response: 184096
[root@logger ~]# pwd
/root
[root@logger ~]#
```

If the correct string is entered, you are connected to the appliance for the amount of time specific to the option you had selected in "Enabling or Disabling SSH Access" on page 34.

Diagnostic Tools

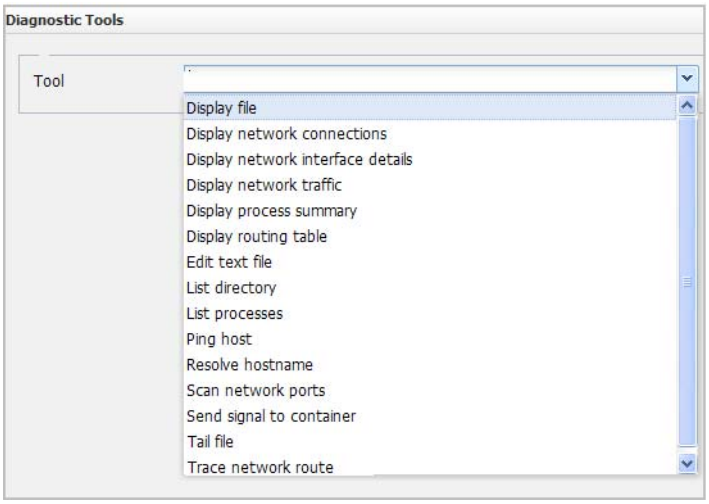
Connector Appliance provides several diagnostic tools that help you set up, manage, and troubleshoot your Connector Appliance. You can run these diagnostics on the local appliance only. To run a diagnostic tool on a remote container, refer to "Running Diagnostics on a Container" on page 129.

To access the diagnostic tools:

1 Click **Setup** > **System Admin** from the top-level menu bar.

2 Click **Diagnostic Tools** from the **System** section in the left panel to open the Diagnostic Tools page.

3 From the Tool drop-down box, select the tool you want to use.



Note

You can start typing the name of the tool you want to use in the Tool drop-down list. Connector Appliance uses character completion to list the tools that contain the characters you type.

4 Enter the required parameters for the tool you selected and click **Run** (click **Edit** for the Edit text file tool).

Each tool, and the parameters and buttons available are described below.

Display file

Use Display file to display the contents of a file. This tool is equivalent to the UNIX command `cat`.

The Display file tool uses the parameters described in the table below:

Parameter/Button	Description
Category	Select the type of file you want to display.
File	Displays a list of files for the type selected in the **Category** field (described above). Select the file you want to display from the list. **Note**: Appliance models Cx400 do not have any boot log files; selecting **Boot Log** from the **File** list displays an empty pop-up window.
Match Expression	Type an expression to display only lines in the file that match that expression. UNIX regular expressions are supported. **Note**: The expression is case sensitive.
Exclude Expression	Type an expression to exclude lines that match that expression from the display. UNIX regular expressions are supported. **Note**: The expression is case sensitive.
Display	You can limit the number of lines you want to display. • Select **Beginning of file** to limit the display to the number of lines specified in the **Number of Lines** field (described below) starting from the top of the file. • Select **End of file** to limit the display to the number of lines specified in the **Number of Lines** field (described below) starting from the bottom of the file. **Note**: If you select **Beginning of file** or **End of file**, you also need to specify a value in the **Number of Lines** field, described below. To display all the lines in the file, leave both the **Display** and the **Number of Lines** field empty.
Number of Lines	Specify the number of lines you want to display from the beginning or end of the file. If you enter an expression to match or exclude, the display contains or omits the first (if you select Beginning of file) or last (if you select End of file) number of occurrences of that expression. For example, if you enter `TCP` in the **Exclude Expression** field, then select **Beginning of file** from the **Display** drop-down, and enter 10 in the **Number of Lines** field, the display contains the first 10 occurrences of the expression `TCP` found starting from the beginning of the file. **Note**: To display all the lines in the file, leave this field and the **Display** field (described above) empty.

Parameter/Button	Description
Run	Click this button to display the contents of the selected file. The file contents display in a pop-up window.

Display network connections

Use Display network connections to review your network connections and transport protocol statistics. The status information can indicate areas where a protocol is having a problem.

This tool is equivalent to the UNIX command `netstat -pn [-t] [-u] [-w] [a] [-l] [-c]`.

The Display network connections tool uses the parameters described in the table below:

Parameter/Button	Description
Protocol	Leave this field empty to display statistics for all transport protocols or select from these options: • **RAW only** displays raw IP protocol statistics. This option is equivalent to the `netstat` UNIX command option `-w`. • **TCP only** displays TCP protocol statistics. This option is equivalent to the `netstat` UNIX command option `-t`. • **UDP only** displays UDP protocol statistics. This option is equivalent to the `netstat` UNIX command option `-u`.
Connection	Leave this field empty to display information for all non-listening connections or select from these options: • **All connections** displays information for all current connections. This option is equivalent to the `netstat` UNIX command option `-a`. • **Listening connections** displays information for listening connections only. This option is equivalent to the `netstat` UNIX command option `-l`.
Mode	Select **Run Continuously** if you want to poll the network status continuously every five minutes. This option is equivalent to the `netstat` UNIX command option `-c`. When **Run Continuously** is not selected, the network status is polled once.
Match Expression	Enter an expression to display only lines that match that expression in the output. UNIX regular expressions are supported.
Exclude Expression	Enter an expression to exclude lines that match that expression from the output. UNIX regular expressions are supported.
Run	Click this button to display the network connection information. The information displays in a pop-up window.

Display network interface details

Use Display network interface details to display the status of a currently active interface on the appliance. This tool is equivalent to the UNIX command `ifconfig`.

The Display network interface details tool uses the parameters described in the table below:

Parameter/Button	Description
Interface	Select the network interface on the appliance whose status you want to display. **Note**: If you leave this field empty, the status of all active network interfaces display.
Run	Click this button to display the status of the selected network interface. The status displays in a pop-up window.

Display network traffic

Use Display network traffic to monitor packets that are transmitted and received on the network. This tool is equivalent to the UNIX command `tcpdump`.

The Display network traffic tool uses the parameters described in the table below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to monitor.
Match Expression	Enter an expression to show only network traffic that matches that expression in the display; For example, if you specify the expression `echo`, only network traffic from the specified host that includes the expression `echo` is displayed. UNIX regular expressions are supported.
Exclude Expression	Enter an expression to exclude network traffic that matches that expression from the display; For example, if you specify the expression `echo`, all traffic except traffic that contains `echo` will be displayed. UNIX regular expressions are supported.
Run	Click this button to display network traffic between the appliance and the specified host. The information displays in a pop-up window.

Display process summary

Use Display process summary to show a list of the currently running processes and see how long they have been running. This tool is equivalent to the UNIX command `top -b -n 1`.

The Display process summary tool uses the parameters described in the table below:

Parameter/Button	Description
Match Expression	Enter an expression to display only processes that match that expression. UNIX regular expressions are supported.
Exclude Expression	Enter an expression to exclude processes that match that expression from the display. UNIX regular expressions are supported.
Run	Click this button to display the list of currently running processes. The list displays in a pop-up window.

Display routing table

Use Display routing table to see the routes through which traffic flows from the appliance. This tool is equivalent to the UNIX command `ip route`.

The Display routing table tool uses the parameters described in the table below:

Parameter/Button	Description
Destination Host	• Leave this field empty if you want to see the entire IP routing table. • Specify the IP address or hostname of a host to see IP routing information from the appliance to that host.
Run	Click this button to obtain the routing table. The routing table displays in a pop-up window.

Edit text file

Use Edit text file to edit files on the appliance. The Edit text file tool uses the parameters and buttons described in the table below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the type selected in the **Category** field (described above). Select the file you want to edit.
Edit	Click this button to display the file for editing. After editing the file, click **Save** or **Revert**.
Save	Click this button to save the edits you make to the file.
Revert	Click this button to cancel the edits you make to the file. After clicking **Revert**, click **Save** to save the reverted text.

List directory

Use List directory to display the contents of a directory on the appliance. This tool is equivalent to the UNIX command `ls -alh`.

The List directory tool uses the parameters described in the table below:

Parameter/Button	Description
Directory	Specify the directory whose contents you want to display. For example: `/opt/arcsight/appliance`
Run	Click this button to display the directory list. The list displays in a pop-up window.

List processes

Use List processes to display the top CPU processes that are currently running together with memory and resource information. This tool is equivalent to the UNIX command `ps -ef`.

The List processes tool uses the parameters described in the table below:

Parameter/Button	Description
Match Expression	Enter an expression to display only the top processes that match that expression. UNIX regular expressions are supported.
Exclude Expression	Enter an expression to exclude processes that match that expression from the display. UNIX regular expressions are supported.
Run	Click this button to display the list of the top processes. The list displays in a pop-up window.

Ping host

Use Ping host to test if a particular host is reachable across an IP network and to measure the round-trip time for packets sent from the appliance to the host. This tool is equivalent to the UNIX command `ping`.

The Ping host tool uses the parameters described in the table below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to ping.
Run	Click this button to ping the specified host. The ping results display in a pop-up window.

Resolve hostname

Use Resolve hostname to look up a hostname in the Domain Name Server and convert it to an IP address. This tool is equivalent to the UNIX command `host`.

The Resolve hostname tool uses the parameters described in the table below:

Parameter/Button	Description
Hostname	Specify the hostname you want to resolve to an IP address.
Run	Click this button to look up the hostname in the Domain Name Server. The result displays in a pop-up window.

Scan network ports

Use Scan network ports to scan a specific host on the network for open ports. This tool is equivalent to the UNIX command `nmap [-p]`.

The Scan network ports tool uses the parameters described in the table below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose ports you want to scan.
Port Range	Optional. Specify a range of ports you want to scan. Separate port numbers in a range by a dash (-) and individual port numbers by a comma. For example, 80-90, 8080. If you do not provide a port range, all ports on the specified host are scanned. This option is equivalent to the `netstat` UNIX command option `-p`.
Run	Click this button to start scanning ports on the specified host. The result displays in a pop-up window.

Send signal to container

Use Send signal to container to send a terminate command to a container. This tool is equivalent to the UNIX command `kill -severity` (where *`severity`* is either `-15` or `-9`).

The Send signal to container tool uses the parameters described in the table below:

Parameter/Button	Description
Severity	Select the severity of the terminate command you want to send to the container. You can select KILL (UNIX `kill` command option `-9`) or TERM (UNIX `kill` command option `-15`).
Container	Select the container to which you want to send the signal.
Run	Click this button to send the signal. The result displays in a pop-up window.

Tail file

Use Tail file to display the last ten lines of a system, application, or log file. This tool is equivalent to the UNIX command `tail -f`.

The Tail file tool uses the parameters described in the table below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the category selected in the **Category** field (described above). Select the file from which you want to display the last ten lines.
Match Expression	Enter an expression to display only lines that match that expression. UNIX regular expressions are supported.
Exclude Expression	Enter an expression to exclude lines from the display that match that expression. UNIX regular expressions are supported.
Run	Click this button to display the last ten lines of the file you selected. The lines display in a pop-up window.

Trace network route

Use Trace network route to display the specific network route between the appliance and a specified host. This tool is equivalent to the UNIX command `traceroute`.

The Trace network route tool uses the parameters described in the table below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose route you want to trace.
Run	Click this button to display the network route. The information displays in a pop-up window.

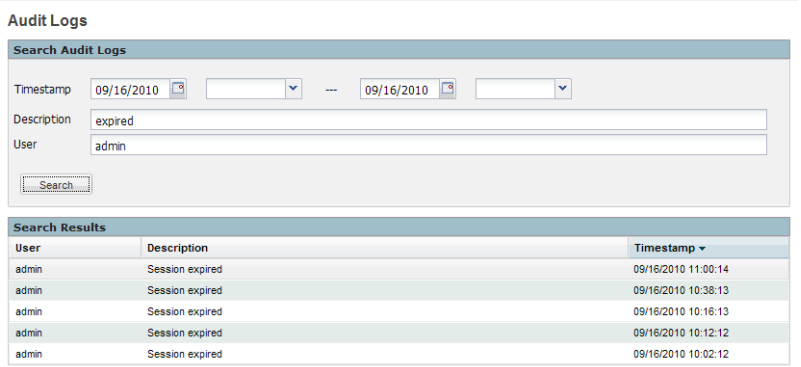
Logs

Your system can generate audit logs at the application and platform levels. Use the Logs sub-menu to search audit logs and configure audit forwarding so that the system can send audit events to a destination, such as ESM.

Audit Logs

Your ArcSight 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. For information about forwarding audit events, see “Audit Forwarding” on page 43.



To view audit logs:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Audit Logs** from the Logs section.
3. Select the date and time range for which you want to obtain the log.
4. To refine the audit log search, optionally specify a string in the Description field and 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 Forwarding

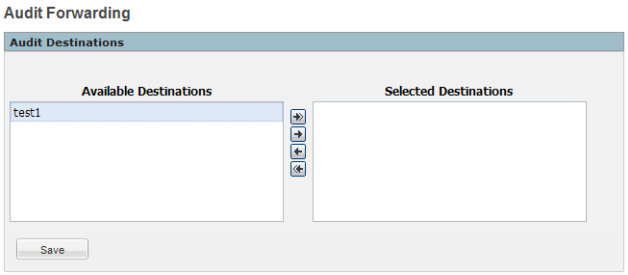
You can forward audit events to ArcSight ESM for correlation and analysis. To configure audit forwarding, you need to have an existing syslog daemon connector configured to the destination where you want to send the audit events.

Each time you re-register a destination for a syslog connector, you have to re-configure audit forwarding.

To forward audit events to specific ESM destinations:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Audit Forwarding** from the Logs section.
3. Select destinations from the Available Destinations list and click the right arrow icon ( ) to move the selected destination to the Selected Destinations list. You can select multiple destinations at the same time and move them over. Or you can move all available destinations by clicking the ( ) icon.

   The destinations are ESM destinations that you configure on the ESM Destinations page (**Configuration** > **Event Input/Output** > **ESM Destinations**).



4 Click **Save Settings**.

Storage

Use the Storage sub-menu to add an NFS mount or a CIFS mount, or SAN (if applicable) and to view the status of the hard disk array (RAID) controller and specific system processes.

Remote File Systems

Your system can mount Network File System (NFS) and CIFS (Windows) shares. As a result, it can read log files and event data from UNIX, Linux, Windows remote hosts, and any Network Attached Storage (NAS) solutions based on these operating systems. You need to establish a CIFS mount before you can add a file-based connector on a Windows system to the Connector Appliance.

Your system supports only NFS v3.0.

Managing a Remote File System

Make sure the following requirements are met before you mount a share.

File System Type	Requirements
CIFS (Windows)	• A user account with read-write privileges to the share exists on the Windows system. • The folder to which you are establishing the mount point is configured for sharing. **Note:** NTLMv2 authentication is supported.
NFS	• Grant your ArcSight system read and write permission on the NFS system. • The account name is ‘arcsight’, but use numeric ids instead: 1500 for uid, or 750 for gid.

To add a Remote File System mount:

1 Click **System Admin** from the top-level menu bar.

2 Click **Remote File Systems** under the Storage section in the left panel.

3 Click **Add** from the top left side of the page and enter values for the following fields in the resulting form.

Parameter	Description
Select File System Type	Choose whether you want to mount an NFS or a CIFS share.
NFS Settings	
Name	A meaningful name for the mount point. The name cannot contain spaces. This name is used locally on your system to refer to the mount point.
Hostname / IP Address	Host name or IP address of the host to which you are creating the mount.
Remote Path (for NFS)	The folder on the remote host that will act as the root of the network file system mount. For example, `/public/system_logs`. Make sure that only this system can write to the location you specify in this field. If multiple systems (or other systems) mount this location and write to it, data on this location will be corrupted.
Mount Options	Autofs options. For example, `ro` for read-only from the remote host, `rw` for read-write, or `hard` to keep retrying until the remote host responds. **Note:** Even if you configure `rw` permission at your mount point, `rw` permission is not granted to the remote host if the host is configured to allow read-only access. **Important**: For log file connectors (for example, the Symantec AntiVirus connector), you need to enable the **directio** option so that Connector Appliance can process new events. Enter `rw,directio` in the **File System Mount Options** field.
Description	A meaningful description of the mount point.
CIFS Settings	
Name	A meaningful name for the mount point. The name cannot contain spaces. This name is used locally on your system to refer to the mount point.
Location	Enter the share name in one of the following ways: • Share name in this format: `IP Address or Hostname: share_name` For example, 198.0.2.160:myshare This folder needs to be configured for sharing. (Typically, to configure a Windows folder for sharing, right click on the folder name > Properties > Sharing.) • UNC path For example, //198.0.2.160:/public/myshare

Parameter	Description
Mount Options	Autofs options. For example, `ro` for read-only from the remote host, `rw` for read-write, or `hard` to keep retrying until the remote host responds. **Note:** Even if you configure `rw` permission at your mount point, `rw` permission is not granted to the remote host if the host is configured to allow read-only access. Important: For log file connectors (for example, the Symantec AntiVirus connector), you need to enable the directio option so that Connector Appliance can process new events. Enter rw,directio in the File System Mount Options field.
Description	A meaningful description of the mount point.
Credentials for CIFS	
Username	Name of the user account with read-write privileges to the Windows share. Make sure the username is prefixed with the domain information. For example, `tahoe/arcsight`.
Password	Password for the user name specified above.

4 Click **Add**.

All mount points are created under `/opt/mnt`. Note the name of the mount point you create. You need to specify this name when adding a connector that will use this share to the Connector Appliance.

To edit a Remote File System mount:

You cannot edit a mount point if it is in use. The edit link is not displayed if the mount point cannot be edited.

If you rename a mount point, access to the archives that were made using the original name is lost until you revert the mount point name to the original name.

1 Click **System Admin** from the top-level menu bar.

2 Click **Remote File Systems** under the Storage section in the left panel.

3 Select the mount point you want to edit and click **Edit** from the top left side of the page.

4 Change the field values.

5 Click **Save**.

To delete a Remote File System mount:

You cannot delete a mount point that is in use. Once stopped, expect up to a two minute delay before the mount can be edited or deleted.

The **Delete** link is displayed only if the mount point can be deleted.

1 Click **System Admin** from the top-level menu bar.

2 Click **Remote File Systems** under the Storage section in the left panel.

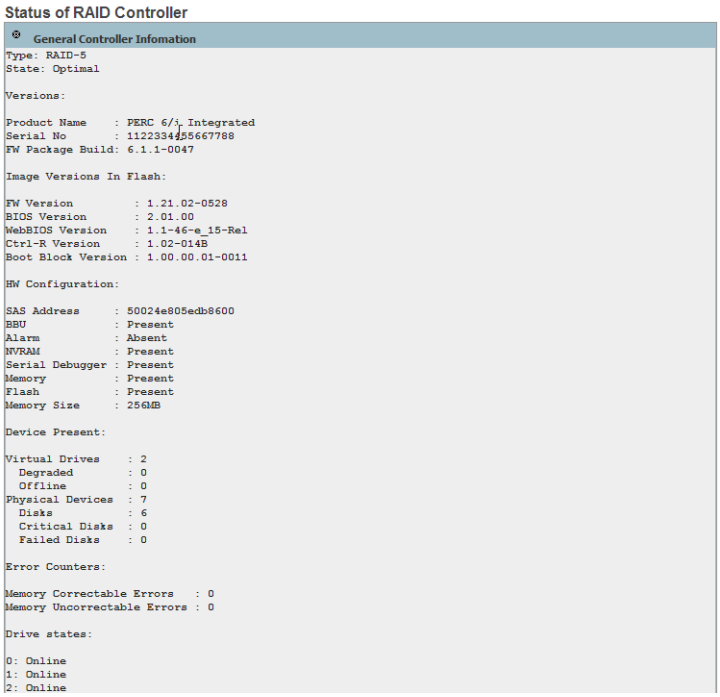
3 Select the mount point you want to delete and click **Delete** from the top left side of the page.

RAID Controller/Hard Disk SMART Data

1 Click **System Admin** from the top-level menu bar.

2 Click **RAID Controller** under the Storage section in the left panel to display a page similar to the one shown in the following figure.

The information displayed depends on the hardware model of your system.



This information is not needed during normal system operations, but it can be helpful for diagnosing specific hardware issues. Due to the redundant nature of RAID storage, unit failure does not disable your system. Instead, performance degrades. Use this report to determine whether a performance issue is caused by a disk failure. ArcSight Customer Support can use this information to better diagnose problems, as well.

On models C1xxx, C3xxx, C13xx, and C32xx the Hard Disk SMART Data menu item displays in the left pane instead of the RAID Controller menu item. Click **Hard Disk SMART Data** from the Storage section in the left pane to display diagnostic information from the hard drive.

FTP

Blue Coat Proxy SG connectors support multiple ways to deliver their log files to the appliance. This section details how to enable the use of FTP for this purpose (For details on other methods, refer to the *SmartConnector Configuration Guide for Blue Coat Proxy SG*). The default for having FTP enabled is **disabled**. In order to use this protocol, you need to enable it on the appliance and set a maximum directory size for the accumulated files. You can perform these steps, as well as manage subdirectories and passwords, from the FTP page shown below.

To enable FTP,

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **FTP** from the **Storage** section.
3. From within **FTP Settings**, check the **Enable FTP** check box.
4. Enter a maximum directory size. When doing so, keep the following in mind:
   - The maximum directory size cannot be greater than that allowed on your appliance model (see "Models Supporting FTP" on page 50). You may change the maximum size at any point, as long as the new size is greater than the total size of all currently stored data.
   - If the maximum you have set is exceeded, FTP stops automatically.
   - Once the file limitation is back within range, FTP automatically restarts.
5. Enter a password.

Anonymous FTP is not supported.

6. Click **Save**.

- Only file put operations are supported by the FTP server. There is no capability to retrieve data from the appliance.
- Data is processed faster and more efficiently when transferred in many small files in lieu of fewer large files.

Adding a Subdirectory

Based on naming convention, incoming log files from different devices can potentially conflict within the same directory. To prevent this, you can create subdirectories to separate them. This window also shows the current size of the subdirectory.

Tip

Creating subdirectories is a good practice, as it allows you to verify how much space is being used and to easily delete subsets of file data.

To add files to the subdirectory,

1. From within the appliance, go to **Setup > System Admin > FTP**.
2. In the **Subdirectory** window, click the **Add** button to name the subdirectory.

   The name appears in the window and displays its current size.
3. From the BlueCoat device's configuration page, enter only the subdirectory name in the **Path:** field, then complete the device's configuration.

Note

When naming subdirectories, the standard Linux directory naming conventions apply.

Receiving log data input via FTP

Receiving input from a connector via FTP requires that some steps be performed outside of the appliance. The following steps allow for the successful transfer of log data.

1. Enable FTP on the appliance. For instructions, see "FTP" on page 48.
2. Configure the SmartConnector. For instructions on how to do this, see the *SmartConnector Configuration Guide for Blue Coat Proxy SG*.

Tip

When configuring the BlueCoat SmartConnector for use with FTP, set up the SmartConnector to delete files after processing. This step helps to prevent an over accumulation of files on the FTP server.

To do so, from within the `agent.properties DeleteFile`, change `agents[0].foldertable[0].mode=`**`RenameInSameDirectory`** to `agents[0].foldertable[0].mode=`**`DeleteFile`**.

Tip

When configuring the BlueCoat SmartConnector for use with FTP, point the connector to `/opt/arcsight/incoming/<or subdirectory>`.

3 Configure the device. For instructions on how to do this, see the documentation for your device.

Models Supporting FTP

The following table lists the Connector Appliance models that support the use of FTP. It can also assist in determining the maximum directory size allowed for storing FTP files.

Model Name	Maximum Directory Size (MB)
C1300	102,206 (95 GB)
C5400	293,348 (235 GB)
C5100	286,277 (240 GB)
C5200	245,854 (240 GB)
C3400	246,568 (275 GB)
C3200	241,183 (285 GB)

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 CAC support.

SSL Server Certificate

Your system uses Secure Sockets Layer (SSL) technology to communicate securely over an encrypted channel with its clients—users, SmartConnectors when using the SmartMessaging technology, and other ArcSight systems. Your system ships with a self-signed certificate. Although you can use this certificate, ArcSight strongly recommends using a CA-signed certificate.

To facilitate obtaining a CA-signed certificate, your system can generate a Certificate Signing Request. Once a signed certificate file is available from the CA, it can be uploaded to your system for use in subsequent authentication.

Your system generates an audit event when the installed SSL certificate is going to expire in less than 30 days or has expired. The event with Device Event Class ID “platform:407” is generated periodically until you replace the certificate with the one that does not expire within 30 days. For more details about this event, see the Audit Logs appendix at the end of this book.

Generating a Certificate Signing Request

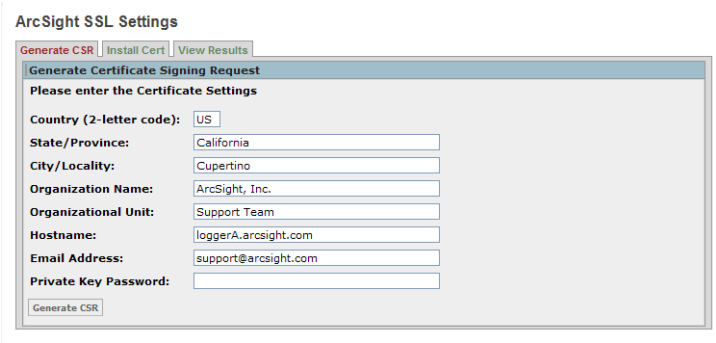
The first step in configuring an SSL certificate is to generate a Certificate Signing Request (CSR). The CSR must be generated on the system for which you are requesting a certificate. That is, you cannot generate a CSR for System A on System B or use a third-party utility to generate it.

The resulting CSR should be sent to a CA, such as VeriSign, which responds with a signed certificate file.

To generate a certificate signing request:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **SSL Server Certificate** from the Security section in the left panel to display the Generate Certificate Signing Request page.



3 In the **Generate CSR** tab, 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 'Cupertino.'
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. Additionally, this name must be identical to the host name specified in "NICs" on page 29. **Note:** If the host name or IP address of this system changes in future, you must generate a new CSR, obtain a new certificate, and upload it .
Email Address	The email address of the administrator or contact person for this CSR.
Private key password	The password to secure the private key on the appliance. This password is not included in the generated CSR. It is stored locally on your system.
Private Key Length	Select the length (in bits) of the private key: 1024, 2048, or 4096.

4 Click **Generate CSR** to generate a Certificate Signing Request.

Installing a Signed Certificate

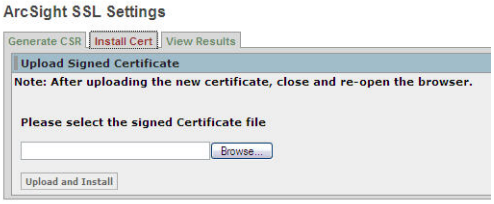
After you have obtained a signed certificate, you need to install the signed certificate file on your system.

To install a signed certificate:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **SSL Server Certificate** from the Security section in the left panel.

3 On the **Install Cert** tab, click **Browse** to find the signed certificate file on your local file system.



4 Click **Upload and Install** to install the specified certificate.

Certain browsers require that you close your current browser and restart it for the new certificate to take affect. If you are aware of this requirement for your browser or are unsure of it, restart your browser.

Viewing Certificate Installation Results

Click the **View Results** tab to display the results of the most recently installed certificate.

SSL Client Authentication (CAC 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 (user name and password), RADIUS, and LDAP 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.

To configure Connector Appliance to support CAC, you need to upload a trusted certificate and a certificate revocation list (CRL), and enable client authentication.

Uploading Trusted Certificates

A trusted certificate is used to authenticate users that log in to your system. The certificate needs to be in Privacy Enhanced Mail (PEM) format.

To upload a trusted certificate:

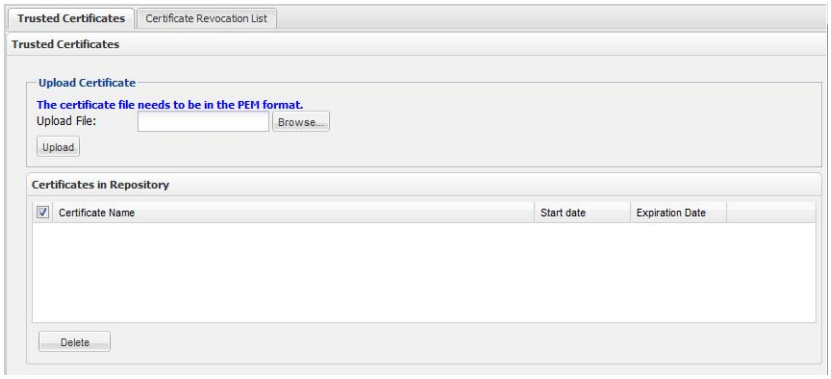
1 Click **System Admin** from the top-level menu bar.

2 Click **SSL Client Authentication** from 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 the **Delete** button.

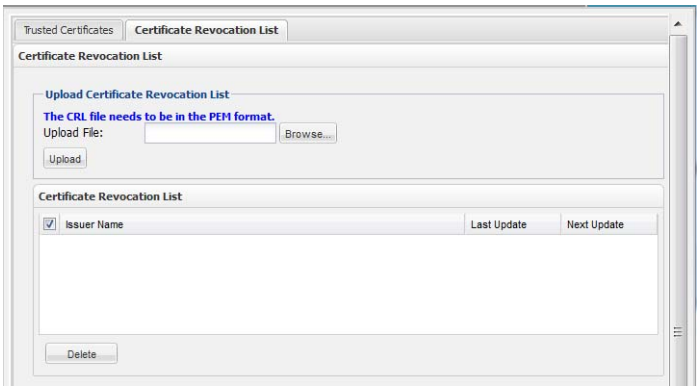
Uploading a Certificate Revocation List

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 **System Admin** from the top-level menu bar.
2. Click **SSL Client Authentication** from 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 Authentication

To enable client certificate authentication, see “Client Certificate Authentication” on page 57.

FIPS 140-2

Your system supports the Federal Information Processing Standard 140-2 (FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards.

If your system needs to be FIPS 140-2 compliant, you can enable FIPS on it. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS 140-2 for all encrypted communication between its internal and external components.To be fully FIPS 140-2 compliant, all components that work together need to be in FIPS mode. When you enable FIPS on the Connector Appliance, the appliance becomes FIPS enabled and meets the standards for cryptographic algorithms defined by the NIST. However, you still need to enable FIPS mode on the containers. Refer to “Enabling and Disabling FIPS on a Container” on page 116.

To enable or disable FIPS mode on the Connector Appliance:

1. Click **Setup** > **System Admin** from the top-level menu bar.
2. Click **FIPS 140-2** from the Security section in the left panel.

If you have just rebooted the appliance, wait 5 minutes before clicking **FIPS 140-2** so that the system has time to load the FIPS page.

3. Click **Enable** or **Disable** in the Configure FIPS Mode area.
4. Click the **Save** button.
5. If the System Reboot Required message displays, click the **System Reboot** link.
6. Check that the appropriate CA certificates are present in the trust store so that connectors can validate their destinations (ArcSight ESM or Logger) successfully. If the appropriate CA certificates are not in the trust store, you need to add them. For information on viewing and adding certificates, see “Running a Command on a Container” on page 125.

   The FIPS Status Table shows which applications and servers are FIPS enabled.

Users/Groups

Use the **Users/Groups** sub-menu to configure Connector Appliance users and user groups, and to set authentication options.

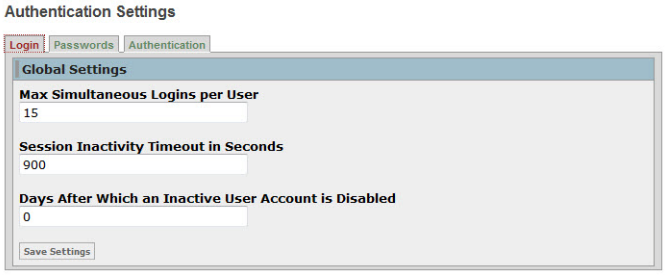
Authentication

The Authentication settings enable you to specify settings and policies for login, password, and the authentication mechanism to use.

Login

The Login (Global) Settings page lets you specify the maximum number of simultaneous sessions for a single user account.

The form, shown in the following figure, also lets you specify how many seconds of inactivity to allow before automatically ending the current session. The default is 900 (15 minutes).



To change login settings:

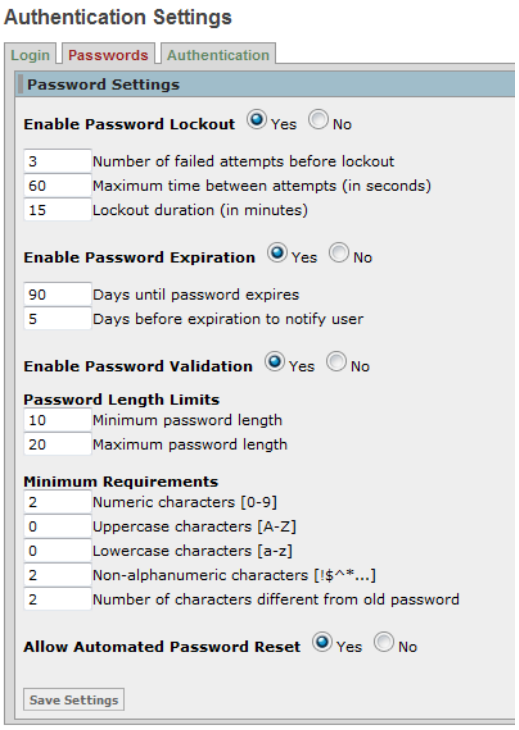
1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Authentication** from the **Users/Groups** section.
3. On the **Login** tab, update the parameters described in the following table.

Parameters	Description
Max Simultaneous Logins per User	The maximum number of simultaneous sessions allowed for a single user account (this helps ease denial of service attacks). The default is 15.
Session Inactivity Timeout in Seconds	How many seconds of inactivity to allow before automatically ending the current session. The default is 900 seconds (15 minutes). **Note**: On a slow network or when Connector Appliance is under heavy load, upgrade operations might be interrupted by a session timeout. Increase the session timeout to prevent this interruption. **Note**: 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.
Days After Which an Inactive User Account is Disabled	The number of days after which Connector Appliance disables an inactive user. The default value is 0.

4. Click **Save Settings** to make the changes, or click another tab or sub-menu to cancel.

Passwords

The Passwords tab enables you to set password policies such as the minimum and maximum number of characters and other requirements for passwords.



To change the password settings:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Authentication** from the Users/Groups section.
3. In the **Passwords** tab, update any or all of the parameters listed in the following table:

Parameter	Description
Enable Password Lockout	Choose **Yes** to enforce the password policy as defined by the following three settings. The default is **No**.
Number of failed attempts before lockout	Default is **3**.
Maximum time between attempts (in seconds)	Default is **60**, or one minute.
Lockout duration (in minutes)	Default is **15**.
Enable Password Expiration	Choose Yes to expire passwords automatically. The default is **No**.
Days until password expires	The default is **90**.

Parameter	Description
Days before expiration to notify user	The default is **5**.
Enable Password Validation	Choose Yes to enforce the length limits and other requirements for new passwords. The default is **No**.
Minimum password length	Enter the minimum number of characters in a password. The default is **10**.
Maximum password length	Enter the maximum number of characters in a password. The default is **20**.
Numeric characters	Enter the minimum number of numeric characters (0-9) in a valid password. The default is **2**.
Uppercase characters	Enter the minimum number of uppercase characters (A-Z) in a valid password. The default is **0**.
Lowercase characters	Enter the minimum number of lowercase characters (a-z in a valid password. The default is **0**.
Non-alphanumeric characters	Enter the minimum number of characters that are not digits or letters that are required in a valid password. The default is **2**.
Number of characters different from old password	The default is **2**.
Allow Automated Password Reset	Enables the “Forgot Password” link on the Login screen that enables users to reset their own password if they forget them. The default is **No**.

4 Click **Save Settings** to make the changes, or click another tab or sub-menu to cancel.

Authentication

Besides providing local authentication, your system supports optional RADIUS, LDAP, and client certificate authentication. You cannot enable all authentication methods at the same time. If any of these methods have the “Allow password fallback” setting set to Yes, local authentication is used.

Client Certificate Authentication

Even if SSL client certificate authentication is enabled on the system, a user name must be defined on it for users to connect to it. See “Users” on page 61 for specifics about setting up a user name for client certificate authentication.

The default ‘admin’ user is exempt and can log on without a certificate even if client certificate authentication is configured on your system.

All SSL client certificates used for authentication must be FIPS compliant (that is, hashed with FIPS compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate authentication:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Authentication** from the Users/Groups section.

3 In the **Authentication** tab, update any or all of the parameters listed in the following table.

Parameter	Description
Use client certificate	Select **Yes** to enable client certificate authentication. Default: **No**
Require additional password	Select **Yes** to require a password in addition to a client certificate for authentication. This is the password configured for a user's name on your system. (See "User Management" on page 60 for more information.) Default: **No**
Allow password fallback	Select **Yes** if a user should be allowed to log in to your system using local password when a certificate is not available or is invalid. Default: **No**

4 Click **Save Settings**.

You must reboot your system for the changes to become effective. See "Reboot" on page 28.

RADIUS Authentication

A user name must exist on your system even if RADIUS authentication is enabled. User name must match the one that exists for the user on the RADIUS server, although passwords can be different. The users must use the RADIUS password to log in.

The default 'admin' user is exempt and can log in even if a RADIUS account does not exist.

To configure RADIUS authentication settings:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Authentication** from the Users/Groups section.

3 In the **Authentication** tab, update any or all of the parameters listed in the following table.

Parameter	Description
Use RADIUS authentication	Select Yes to enable RADIUS authentication. Default: **No**
Allow local password fallback	Select **Yes** if a user should be allowed to log in to your system using local password when RADIUS authentication fails or is not available. Default: **No** Note: The default 'admin' user is exempt and can log in even if this option is set to No.
RADIUS server hostname[:port]	The host name and port of the RADIUS server.
Shared authentication secret	The RADIUS passphrase.
NAS IP Address	The IP address of the Network Access Server (NAS).

Parameter	Description
Request timeout (in seconds)	Length of time to wait for a response from the RADIUS server (in seconds). Default: **10**.
Number of retries	Number of times to retry a RADIUS request. Default: **1**.

4 Click **Save Settings**.

5 Reboot your system for the changes to become effective. See "Reboot" on page 28.

LDAP/AD Authentication

A user account for each user must exist locally on your system even if LDAP authentication is enabled. 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 specified on the LDAP server.

The default 'admin' user is exempt and can log in even if an LDAP account does not exist.

To configure LDAP authentication settings:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Authentication** from the Users/Groups section.

3 In the **Authentication** tab, update any or all of the parameters listed in the following table.

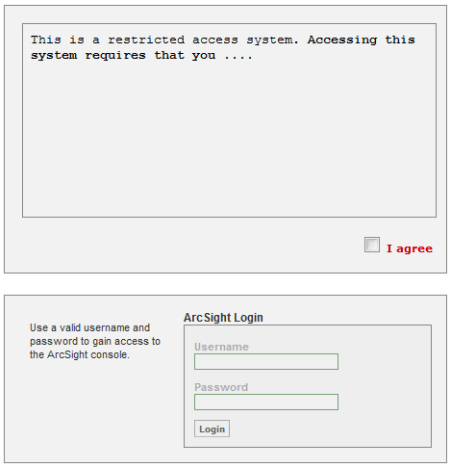
Parameter	Description
Use LDAP/AD authentication	Select Yes to enable LDAP authentication. Default: **No**
Allow local password fallback	Select **Yes** if a user should be allowed to log in to your system using local password when LDAP authentication fails or is not available. Default: **No** Note: The default 'admin' user is exempt and can log in even if this option is set to No.
LDAP server hostname[:port]	The host name or IP address and port of the LDAP server in this format: ldap://<hostname or IP address>:<port>
Backup LDAP Server Hostname[:Port]	(Optional) The backup LDAP server to use if the primary server does not respond. This server is not tried if an authentication request to the primary server fails. Use the same format as the primary server to specify the host name and port.
Request timeout (in seconds)	Length of time to wait for a response from the LDAP server (in seconds). Default: **10**.

4 Click **Save Settings**.

You must reboot your system for the changes to become effective. See “Reboot” on page 28.

Login Banner

You can customize the message on the login screen to suit your needs. The message you enter is displayed above the Username and Password fields on the login screen, as shown in the following figure. The message can only contain text; you cannot include images in it.



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 your login banner:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **Login Banner** from the Users/Groups section.

3 Enter the text you want to display as the login banner in the Content field.

You can only enter 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 a confirmation string in the Confirmation field.

If you enter a string in this field, it inserts a check box that the user must click to enable the Username and Password fields. For example, you can enter “Are you sure?”, “Do you want to proceed?”, or “I agree” in this field if the users of this system must confirm their intent before proceeding further.

5 Click **Save**.

User Management

Use the Users and Groups tabs to manage the users and user groups on your system. User groups are a way to enforce access control to various sections of your system.

Users

Use 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.

Reset Password

You can also reset the password of a user without knowing their password using the reset password feature. Using an SMTP configured server, you can reset a user's password by clicking the **Reset Password** button. An automated email is sent to the user with the new password string. The user must use this temporary string to login within the time specified in the email. If the user does not log in within the specified time, an admin user can reset their password again to generate another temporary password. The user must be activated before resetting the password.

Users can be activated by editing and checking the active flag, then saving the changes.

To add a new user:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **User Management** under 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	A login name for the user.
Password	A password for the user.
Confirm Password	Reenter the password.
Contact Information	

Use Client DN	If you enabled SSL client authentication or LDAP authentication, click this link to enter the Distinguished Name (Certificate Subject) information for the user. Distinguished Name should be similar to this format:
	`/ST=California/C=US/L=Cupertino/O=ArcSight, Inc./OU=Engg Team/CN=UserA/D/emailAddress=email@xyz.com`
	To determine the DN, use this URL to display the certificate:
	`https://<hostname or IP address>/app/cert`
	OR
	Obtain the DN information for a user from the browser that the user will use to connect to the system. For example, on Firefox, click **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates** > **Your Certificates** > Select the certificate > **View**.

First Name	First name of the user.

Parameter	Description
Last Name	Last name of the user.
Email	An email address for the user.
Phone Number	Phone number for the user. (Optional)
Assign to Groups	
System Admin Connector Appliance Rights	Select **Default System Admin Group** from the System Admin drop-down box to give the user rights to change the settings in the System Admin menu. Select **Default Connector Appliance Rights Group** from the Connector Appliance Rights drop-down box to give the user rights to view the **Monitor** tab and access the **Backup/Restore** menu. **Note**: Select both **Default System Admin Group** from the System Admin drop-down box and **Default Connector Appliance Rights Group** from the Connector Appliance Rights drop-down box to display all the tabs and menus.

5 Click **Save and Close**.

To edit a user:

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **User Management** under 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:

A system admin level user account that has been used to upgrade the system cannot be deleted. For example, if system admin user Joe upgrades the system, Joe's user account can not be deleted from the system once the upgrade is complete. To remove such a user, disable the user account. To disable a user account, edit the user account and disable the "Active" option.

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **User Management** under 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.

To reset the password of a 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.

1 Click **Setup > System Admin** from the top-level menu bar.

2 Click **User Management** under 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.

Groups

User groups define privileges to specific functions on your ArcSight system and are the way 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, you could assign that user to the System Admin group, but not the Connector Appliance group.

User groups are organized by the following types: Connector Appliance Rights Groups and System Admin 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 only enable the privileges you want to provide, then assign restricted users to the newly created group.

Connector Appliance Rights Groups

The Connector Appliance Rights Group controls the Connector Appliance application operations for your ArcSight system, such as viewing the Connector Appliance dashboards and backup operations.

Read Only Connector Appliance Group

In addition to the Default Connector Appliance Rights Group that enables all privileges, Connector Appliance now provides more controlled authorizations and a “view only” default option. A read-only user can view the tabs and the operations within the tabs, as well as certain operations such as refresh, view certificate list, and logfu.

Refer to your system’s user interface to see a complete list of rights (privileges) available in this group.

In the **Default Connector Appliance Group**, under “Application Options”:

- Option rights can now be found here, not under System Admin Groups.
- Two new management rights (or privileges) allow for control of the “Manage” and “Repositories” tabs.

System Admin Groups

The System Admin Group controls the system administration operations for your ArcSight 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 exists on your system. Users assigned to this group can only view the System Admin settings, but not change them.

Refer to your system’s user interface to see a complete list of privileges available in this group.

Managing a User Group

To create a new user group:

1 Click **System Admin** from the top-level menu bar.

2 Click **User Management** under 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 **System Admin** from the top-level menu bar.

2 Click **User Management** under 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, as shown in the following figure.

   b Click **Add** from the top left of the Edit Group Membership page.

   c Select users you want to add. By default, you can only add users who do not belong to other groups of the type that you are editing. However, if you want to add such users, click **Show users that belong to other <group_type> groups**, as shown in the following figure. *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 **System Admin** from the top-level menu bar.

2 Click **User Management** under 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

Use the Change Password menu to change your password. This feature is available to all ArcSight system users for changing their passwords, unlike the Reset Password feature that enables a system administrator to reset the password of system users without knowing their passwords.

To change your password:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Change Password** under 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**.

Passwords are subject to the password policy specified by the Admin user. See "Passwords" on page 56.

Forgot Password

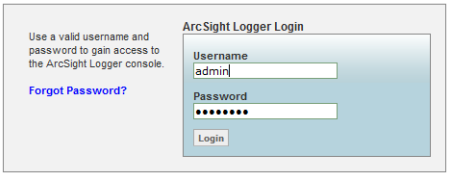
If you forget your system password, use this feature to obtain an email that provides a temporary password. The email address can be applied in the user settings for the user name you specify for obtaining the temporary password.

The temporary password is only valid until the time specified in the email. If you do not login within the specified time, only an administrator can reset the password to generate another temporary password.

This feature is only available if the "Allow Automated Password Reset" setting on the Authentication Settings page (System Admin > Authentication) is set to **Yes**. By default, this setting is set to **No**. Additionally, an SMTP server must be configured on the system for this feature to work successfully. If an SMTP server is not set, you will not be able to reset the password because the email containing the temporary password cannot be sent.

To reset your password:

1. Click the **Forgot Password** link on the Login screen as shown in the following figure.



2. Enter the name of a user in the Username field on the Reset Password screen. Click **Reset Password**.

   An automated email with a temporary password is sent to the email address specified in the user settings of the user you entered.

Chapter 5

Backup and Restore

The following topics are discussed here:

Backup and Restore

The Backup and Restore menu item enables you to backup and restore the Connector Appliance configuration and to retrieve Connector Appliance logs.

Appliance Backup

You can back up the current Connector Appliance configurations as often as needed to a remote system on the network or to your local system.

To back up the configuration:

1. Click **Setup** > **Backup/Restore**.
2. Click **Appliance Backup** from the left panel.
3. Enter 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.
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.
Backup	• Select **All** to create a backup file that contains all data and configuration settings on the appliance. This includes connector data stored in the cache and all files stored in the repositories. • Select **Exclude Connector Data** to create a backup file that contains all data and configuration settings on the appliance, including all files in the repositories, but does not include connector data stored in the cache. • Select **Exclude Repository Data** to create a backup file that contains all data and configuration settings on the appliance, including all connector data stored in the cache, but does not include files in the repositories. • Select **Exclude Connector and Repository Data** to create a backup file that contains all data and configuration settings on the appliance, but does not include connector data stored in the cache or files stored in the repositories. Selecting this option creates a smaller backup file.

4. Click **Save** to back up the configuration.

   If you selected **Save to Local**, follow the steps according to your browser to download the file to your local disk.

Appliance Restore

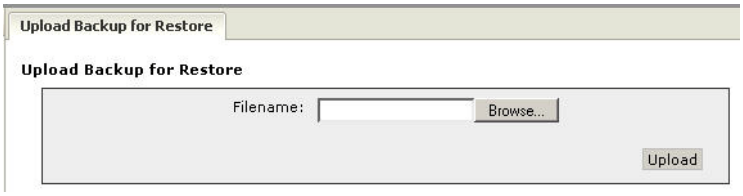
You can restore the appliance configuration from a previous backup.

To restore the configuration:

1 Click **Setup** > **Backup/Restore**.

2 Click **Appliance Restore** from the left panel.

3 Click **Browse** and select the file.



4 Click **Upload** to restore the configuration from the specified backup file.

Caution

The version of the appliance used to restore the backup and the version of the appliance used to create the backup must be the same.

You can only restore a backup to the same appliance from which you created the backup.

5 Re-import the SSL certificate for each container. Click the  icon to run the Certificate Download wizard and import the valid certificates.

Note

After restoring the appliance configuration:

- The cache size on the restored appliance 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 restored appliance might be different from those in the backup file.
- It might take a few minutes before the Cache column on the Connectors page displays the updated cache size for the connectors.

Appliance Snapshot (Logs)

The Connector Appliance records some audit and debug information, including details of any issues that occur. Like the *black box* on an airliner, these system logs create a snapshot of your Connector Appliance activity. If the appliance encounters a problem, the logs can be helpful. The log file retrieved is a `.zip` archive of several log files.

ArcSight Customer Support sometimes asks you to retrieve system logs as part of an incident investigation. To retrieve system logs, follow the steps below and upload the resulting `.zip` file to ArcSight Support.

To retrieve system logs:

1. Click **Setup** > **Backup/Restore**.
2. Click **Appliance Snapshot** from the left panel.

   The Retrieve Snapshot Status page displays.
3. Click the **Download** button.

Chapter 6

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 the logs require you to load the logs to a Log repository. You can also maintain centralized repositories for files needed for connector configuration and management.

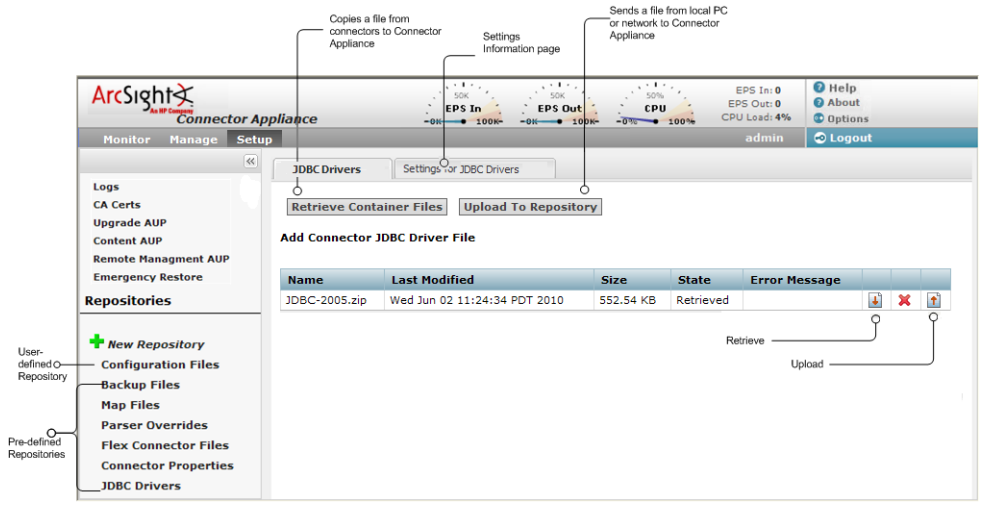


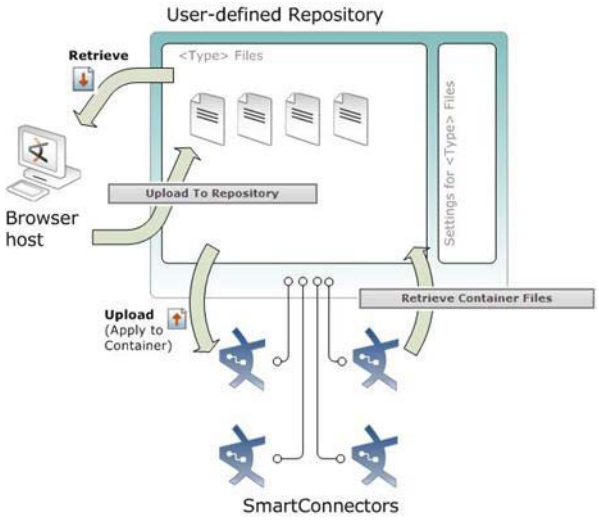
Figure 6-1 Repository Functions

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 connectors 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 connectors.



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
- Manage remote management configuration AUP files in the Remote Management AUP repository
- Restore a container when it is damaged and irrecoverable
- Maintain centralized repositories of files for connector configuration and management

Logs Repository

When you want to view connector logs, you need to first **Load** the logs of the container that contains the connector to the Logs repository, 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 127.

Uploading a File to the Logs Repository

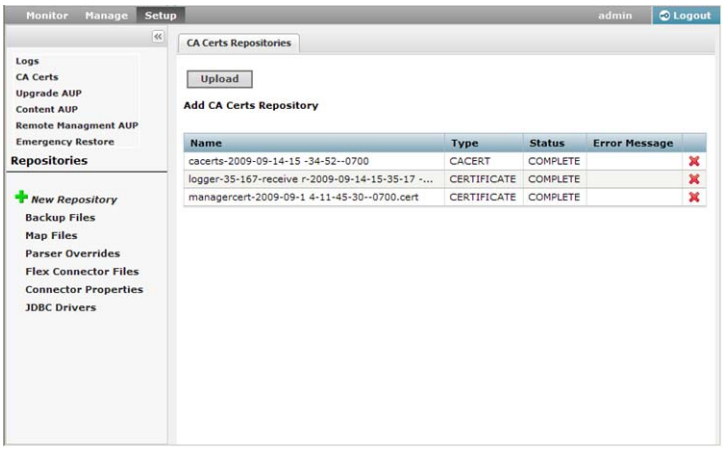
Uploading a file into the Log repository is useful for sharing annotated log or other files with other users. The file needs to be in `.zip` format.

To upload a file:

1. Click **Setup** > **Repositories**.
2. Click **Logs** from the left panel.
3. Click **Upload** from the right 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.



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 117.

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.

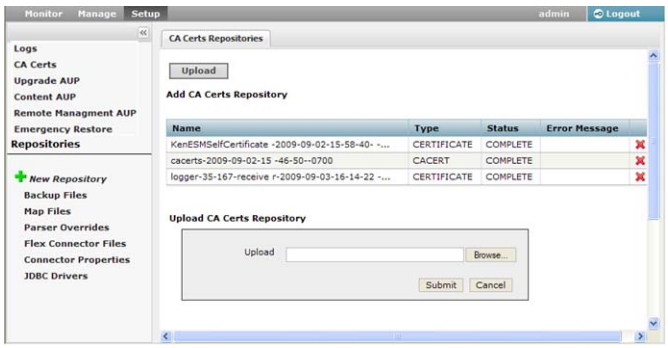
Uploading CA Certificates to the Repository

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 **Setup** > **Repositories**.
2. Click **CA Certs** in the left panel.
3. Click **Upload** in the right panel.
4. Enter the local path for the CA Certs file or the certificate, or click **Browse** to select it.
5. 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

You can delete a CA Certs file or a single certificate 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 117.

To remove a certificate from the repository:

1. Click **Setup** > **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. The central appliance needs to be upgraded using the `.enc` file before you use it to upgrade other appliances remotely.

About the AUP Upgrade Process

The process discussed in this section only applies to upgrading connectors and to upgrading a remotely-managed Connector Appliance. If you are upgrading the local Connector Appliance (localhost), use a `.enc` file. Refer to the Release Notes for more information.

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 126) or to a remote Connector Appliance (see "Upgrading a Host Remotely" on page 110).

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://www.arcsight.com/supportportal 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 **Setup** > **Repositories** from the top-level menu bar.
4. Click **Upgrade AUP** from the left panel.
5. Click **Upload** from the right 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 126.
   - For a remotely-managed Connector Appliance upgrade, see "Upgrading a Host Remotely" on page 110.

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 **Setup** > **Repositories** from the top-level menu bar.
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.

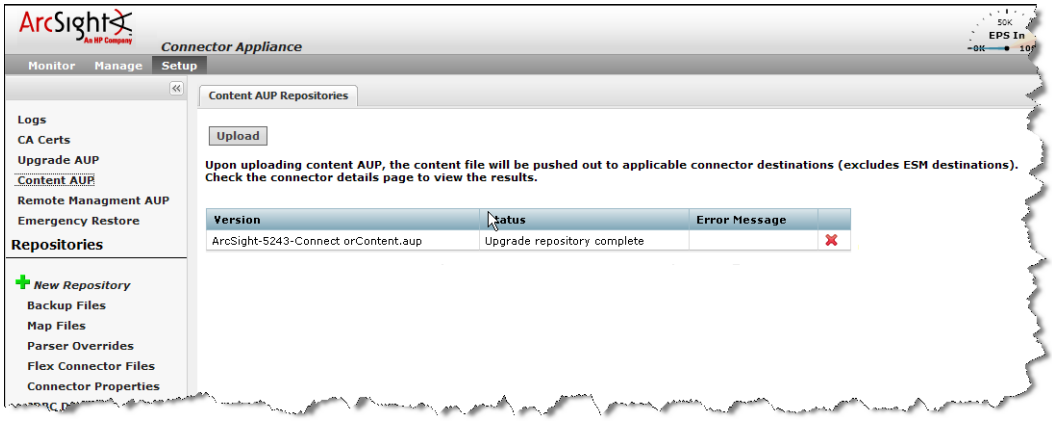
You can maintain a number of Content AUP files in the Content AUP repository. When an AUP file with a version number higher than the ones already in the repository is loaded, it is automatically pushed out to the connector destinations being managed. However, these connectors or connector destinations 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 connectors



To apply a new Content AUP:

1. Download the new Content AUP version from ArcSight Customer Support site at http://www.arcsight.com/supportportal 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 **Setup** > **Repositories** from the top-level menu bar.
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the right 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 connector 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 Destination" on page 151.
- Hover your mouse over a connector 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 **Setup** > **Repositories** from the top-level menu bar.
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.

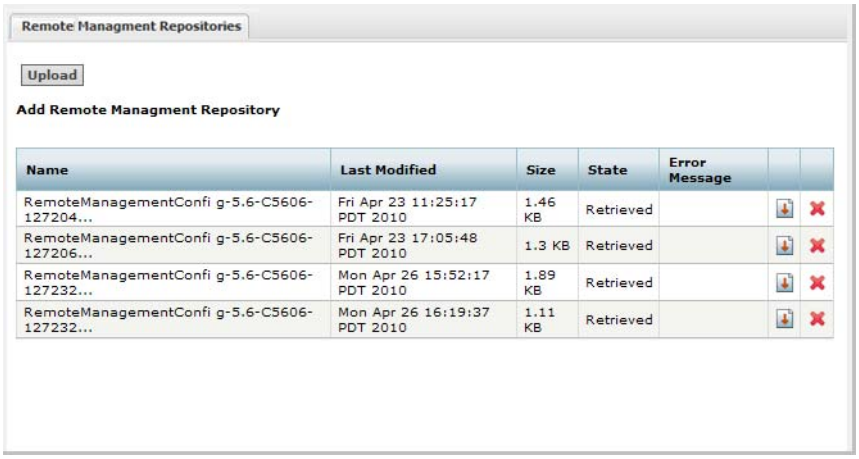
Remote Management AUP Repository

The Remote Management AUP repository stores AUP files that contain the remote management configuration of an appliance (a snapshot of all the remote software connectors and remote Connector Appliances that the appliance manages).

From the Remote Management AUP repository, you can:

- Download a Remote Management AUP file to your local computer (or network host accessible from the local computer) so that you can import the remote management configuration on another appliance.
- Upload Remote Management AUP files from your local computer (or network host accessible from the local computer) to the repository for storage.
- Delete Remote Management AUP files you no longer need.

The following example shows the Remote Management AUP repository.



Downloading Remote Management AUP Files

After you export the remote management configuration of a Connector Appliance, you can download the AUP file that contains the configuration to your local computer (or network host accessible from the local computer) so that it can be imported on another appliance.

For information on exporting and importing the remote management configuration of an appliance, refer to "Exporting and Importing Remote Management Configuration" on page 102.

To download a Remote Management AUP file to your local computer:

1 Click **Setup** > **Repositories** from the top-level menu bar.

2 Click **Remote Management AUP** from the left panel.

3 Locate the AUP file in the table and click next to the file to download it to your local computer.

Uploading Remote Management AUP Files

You can upload remote management AUP files to the Remote Management AUP repository for storage.

To upload a Remote Management AUP file to the repository:

1. Click **Setup** > **Repositories** from the top-level menu bar.
2. Click **Remote Management AUP** from the left panel.
3. Click the **Upload** button at the top of the page.
4. Click **Browse** and select the file you want to upload from the local computer (or network host accessible from the local computer).
5. Click **Submit** to add the specified file to the repository.

Deleting Remote Management AUP Files

When a remote management AUP file is no longer up-to-date or needed, you can remove it from the repository.

To delete a Remote Management AUP file:

1. Click **Setup** > **Repositories** from the top-level menu bar.
2. Click **Remote Management AUP** from the left panel.
3. Locate the AUP file that you want to delete and click the associated  icon. Repeat for multiple files.

Emergency Restore

The Container Restore wizard guides you through the process of restoring a modified container. This feature is supported only for connectors and containers on the local host.

ArcSight recommends that you use this process only when a container is severely damaged and is no longer available. The Emergency Restore process deletes all information about that container and renders it empty. The connector is restored to the AUP version that you select.

To restore a container:

1. Click **Setup** > **Repositories** from the top-level menu bar.
2. Click **Emergency Restore** from the left panel.
3. Follow the instructions in the Container Restore wizard.
4. Re-import the SSL certificate for the container. On the **Manage** tab, click the container name in the left panel. On the **Connectors** tab in the right panel, click the  icon to run the Certificate Download wizard and import the valid certificate.

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 `$ARCSIGHT_HOME/user/agent`, for files to be uploaded or for locations to download files. ArcSight connectors use a standard directory structure, so map files, for example, are always found in `$ARCSIGHT_HOME/user/agent`, (that is, the root directory, `$ARCSIGHT_HOME`, of the connector installation) 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 88).

Files viewed in the user-defined repository can be bulk processed with specified connectors 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 **Setup** > **Repositories** from the top-level menu bar.
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
Restart Connector Process	Check to restart the connector process after file operations.

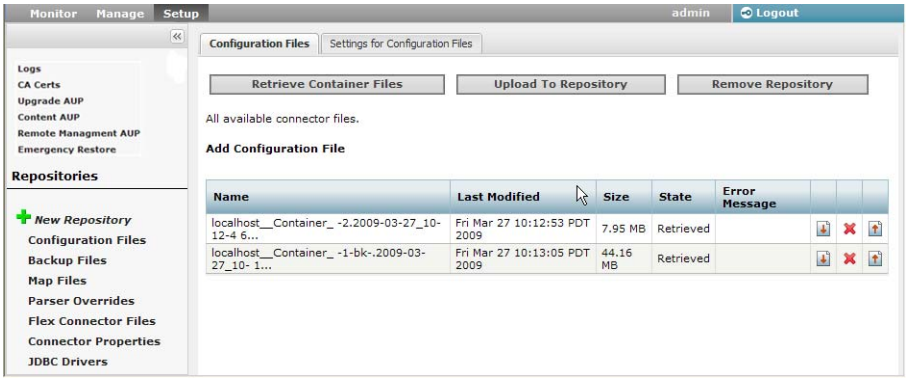
Parameter	Description
Filename Prefix	An identifying word that is included in the names of retrieved files. For example, map files are identified by `Map` in the file name: `localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip`
Relative path (Download)	The path for download, relative to `$ARCSIGHT_HOME`, for example, `user/agent/map` or `user/agent/flexagent`. Leave this field blank to specify files in `$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 connectors to a repository. The specific files that are retrieved depend on the settings of a repository.



To retrieve a container file:

1. Click **Setup** > **Repositories** from the top-level menu bar.
2. In the left panel, click the name of the repository to which you want to copy connector files.
3. Click **Retrieve Container Files** in the right 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 **Setup** > **Repositories** from the top-level menu bar.
2. In the left panel, click the name of the repository to which you want to upload files.
3. Click **Upload To Repository** from the right panel.
4. Follow the instructions in the Repository File Creation wizard.

   Although you can select Repository zip file in the **Select the type of file that you want to upload** page of the Repository File Creation wizard, ArcSight recommends that you 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 **Setup** > **Repositories** from the top-level menu bar.
2. From the left panel, click the name of the repository you want to delete.
3. Click **Remove Repository** from the right 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 **Setup** > **Repositories** from the top-level menu bar.
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 right 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 network), 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 **Setup** > **Repositories** from the top-level menu bar.
2. From the left panel, click the name of the repository in which the file exists.
3. Click  from the right 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 **Setup** > **Repositories** from the top-level menu bar.
2. In the left panel, click the name of the repository in which the file exists.
3. In the right panel, click  next 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 **Setup** > **Repositories** from the top-level menu bar.
2. In the left panel, click the name of the repository in which the file exists.
3. In the right 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 94).
- **Map Files**: enrich event data
- **Parser Overrides**: customize the parser (see "Adding Parser Overrides" on page 95)
- **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 right 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

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_).*$

Table 6-1 Pre-Defined Settings for Backup Files

Settings for Map Files

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
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	

Table 6-2 Pre-Defined Settings for Map Files

Settings for Parser Overrides

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	

Table 6-3 Pre-Defined Settings for Parser Overrides

Settings for FlexConnector Files

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	

Table 6-4 Pre-Defined Settings for FlexConnector Files

Settings for Connector Properties

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	
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	

Table 6-5 Pre-Defined Settings for Connector Properties

Settings for JDBC Drivers

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	

Table 6-6 Pre-Defined Settings for JDBC Drivers

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 are appended to the existing contents of the destination container.

Containers on Connector Appliance are pre-installed with the latest connector release. 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 **Manage** from the top-level menu bar to list the containers and determine the source and destination for cloning.
2. Click **Setup** > **Repositories** from the top-level menu bar.
3. Click **Backup Files** under the **Repositories** section in the right panel.
4. 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 87 to retrieve the container's backup file to the Backup repository.

   The retrieved file is named in <*connector name*> ConnectorBackup <*date*> format.
5. Follow the instructions in "Uploading a File from the Repository" on page 87 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 **Setup** > **Repositories** from the top-level menu bar.
2. Click **Parser Overrides** under the **Repositories** section in the right 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 **Setup** > **Repositories** from the top-level menu bar.
2. Click **Parser Overrides** under the **Repositories** section in the right 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 will be deployed in the selected container.

You can download a parser override file from ArcExchange. For more information, refer to "Sharing Connectors (ArcExchange)" on page 159.

To verify that the parser override has been applied successfully, issue a Get Status command to the connector. See "Sending a Command to a Destination" on page 151. In the report that appears, check for the line starting with the text `ContentInputStreamOverrides`.

Chapter 7

Managing Connectors

The following topics are discussed here.

Connector Overview

You can manage the configuration of these kinds of connectors:

- **Local (on-board) connectors**: Pre-installed connectors on the local Connector Appliance.
- **Remote Connector Appliance connectors**: Pre-installed connectors on a remotely-managed Connector Appliance.
- **Software-based connectors**: Software-based connectors installed manually on a remote host.

A connector configuration consists of properties such as name and type, and a set of *parameters* that customize how the connector works in a specific environment. Parameters vary based on the type of connector; for example, a connector for a firewall has different parameters than a connector that reads an intrusion detection system database.

You can manage connectors of many types, including syslog, Simple Network Management Protocol (SNMP), BlueCoat SmartConnector via FTP, specific Intrusion Detection Systems (IDS), log files, vulnerability scanners, and operating system-specific security events. You can view the list of supported types in the drop-down menu when you configure a new connector.

The connectors you manage are configured automatically to run as *services* or *daemons*.

Individual software-based connectors are described in ArcSight documents specific to those connectors, including the connector-specific configuration guides available with each connector. You can also find general connector information in the *SmartConnector User's Guide*. All of these documents are available from the ArcSight Customer Support site.

Navigating the Manage Tab

The Manage tab enables you to configure and organize connectors. This section describes the user interface elements and explains how to use them effectively.

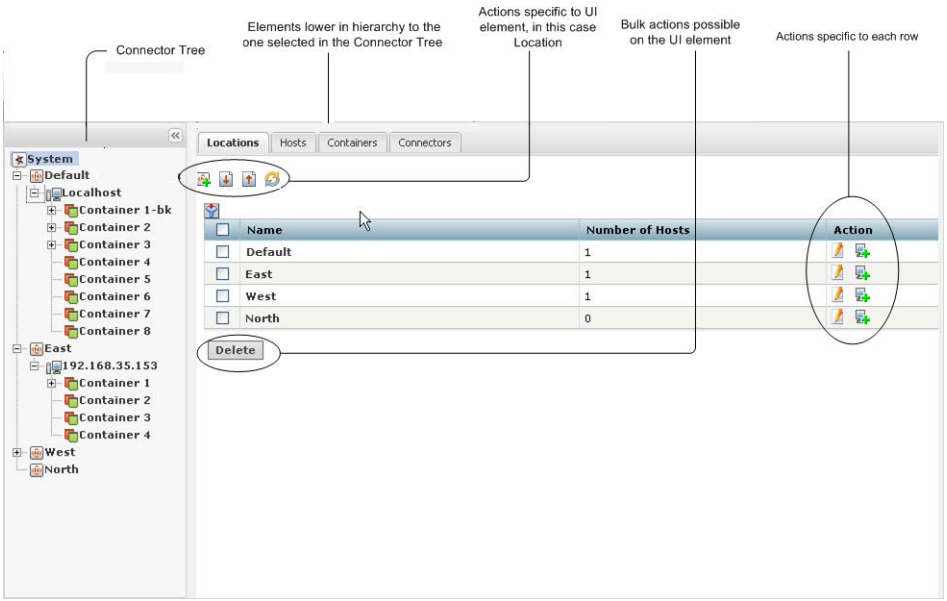
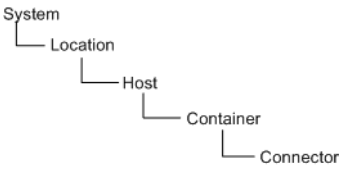


Figure 7-1 Managing Connectors

The Connector tree (the left panel of the window shown in Figure 7-1) organizes connectors into a hierarchy as follows:

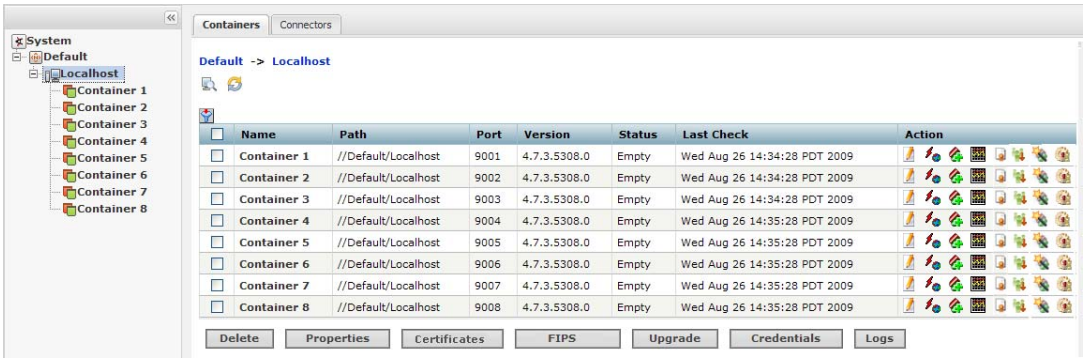


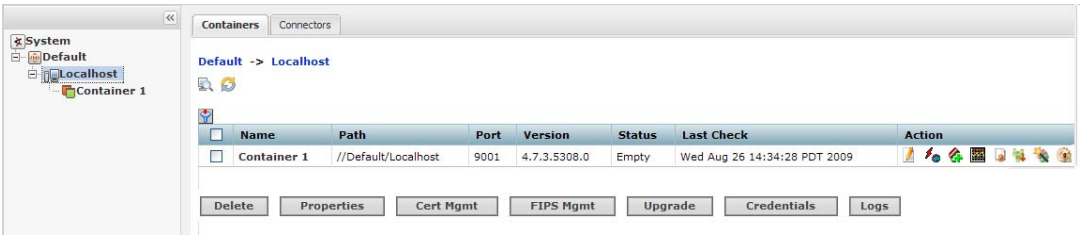
Each connector you manage belongs to a container; each container belongs to a host; each host belongs to a location; and, all locations belong to root of the System.

When you click on an upper-level user interface element in the left panel, the interface displays elements lower in the hierarchy to it on the right panel. You can also perform management operations on the elements displayed on the right side.

For example, **System** provides the root (top-level) view. When you click System, all configured locations are listed in the left panel, as well as under the **Locations** tab in the right panel. You can perform various management tasks, such as editing, deleting, or adding a host, on those locations. In addition, all hosts, containers, and connectors on this system are displayed in specific tabs in the right panel. Click the **Hosts** tab to view all hosts on the system, and click **Containers** and **Connectors** to view the respective elements and perform management operations on them. Similarly, if you select a host (from the left

panel), all containers and connectors configured on that host are displayed on the right panel, as shown in the following figure.





When a container is down or a host is unreachable, the system waits for it to come online. There might be a delay of several minutes before the connector tree (in the left panel) and the Container tab (in the right panel) display.

On any user interface, you can perform three kinds of operations:

- A global operation—Listed on top of a user interface page; for example, you can upload a CSV file of locations.
- A localized operation—An operation on a single element displayed on the user interface page; for example, you can add a connector to a container by clicking the  icon in the Action column in the container's row.
- A bulk operation—A single operation performed on multiple elements on the user interface page; for example, you can upgrade multiple containers by selecting the containers (click the box to the left of the container to select it) and clicking Upgrade at the bottom of the page.

- The  icon refreshes a UI screen. This icon is available on the UI pages when relevant.
- Click the column filter icon () to display drop down lists of values on which to filter each table column. Click the check box in the table header to check or uncheck all check boxes in a single column.
- When processing user provided data, Connector Appliance wizards "escape" some HTML-specific characters. Any other entered characters are not "escaped" (or validated) and are used as entered.

Locations

Location is a logical grouping of hosts. The grouping can be based on any suitable abstraction—geographical, organizational, and so on. For example, you can group all hosts in New York separately from hosts in San Francisco and label them as such. Similarly, you can group a few machines under Sales and others under Marketing.

A location can contain **any number** of hosts. **Default** location is provided on a new Connector Appliance or on a Logger appliance running Connector Manager.

Caution

ArcSight recommends that you do not delete the location **Default**.

You can view all locations on the system and view hosts, containers, and connectors in a location. You can add, edit, and delete a location. You can also add hosts to a location. All these procedures are described below.

Viewing All Locations

You can see all the locations that exist on the system.

To view all locations:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel.

   All existing locations display on the Locations tab in the right panel.

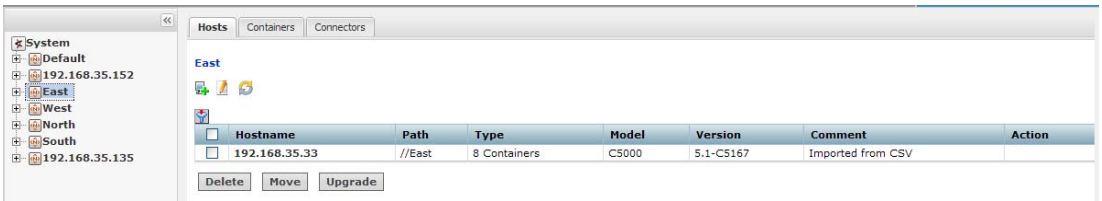
Viewing Hosts, Containers, and Connectors in a Location

You can see all the hosts, containers, and connectors that exist in a location.

To view hosts, containers, and connectors in a location:

1. Click **Manage** from the top-level menu bar.
2. Click the location (listed under System) from the left panel.

   The hosts, containers, and connectors in the location display in the right panel, under specific tabs, as shown below.



Adding a Location

Before adding hosts, you need to add a location, which is a logical grouping of hosts.

You can also add locations in bulk using a comma-separated values (CSV) file. For more information see, Adding Locations and Hosts from a File, below.

To add a location:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel.
3. Click  (on top of the page) in the right panel.
4. Enter the name of the new location and click **Next**.
5. Click **Done**.

Exporting and Importing Remote Management Configuration

You can create a backup of the complete remote management configuration settings on the Connector Appliance (all remote software connectors and remote Connector Appliances that are managed by the appliance) and import the configuration on another appliance.

Local containers are not included in the backup. To back up local containers on the appliance, perform an appliance backup; see “Appliance Backup” on page 28.

The remote management configuration is saved in AUP format in the Remote Management AUP repository so you can download it to your local computer.

You cannot manage the same connectors using two appliances at the same time. Before importing the remote management configuration to another Connector Appliance, you need to shut down the appliance from which you exported the configuration.

You can import the remote management configuration only on the same appliance model as the one from which the configuration is exported. For example, if you export the remote management configuration from a model C5000 appliance, you can import the configuration to a model C5000, C5100, or C5200 appliance. You cannot import the configuration to a model C3100 appliance.

To export the remote management configuration:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel.
3. Click  (on top of the page) in the right panel.
4. Follow the instructions in the * to export the configuration. The remote host configuration is saved in AUP format in the Remote Management AUP repository.

After you export the remote management configuration, you need to download it to your local computer from the Remote Management AUP repository.

After you have exported the remote management configuration and have downloaded it to your local computer, you can import the configuration to another appliance.

Note

Importing the remote management configuration overwrites the current remote management configuration on the appliance.

To import the remote management configuration:

1. On the appliance where you want to copy the remote management configuration, click **Manage** from the top-level menu bar.
2. Click **System** in the left panel.
3. Click (on top of the page) in the right panel.
4. Follow the instructions in the wizard. When selecting the type of upload, choose **Full remote management (AUP format)**.

Note

If there are no valid CA certificates for any connectors in the configuration, you see a question mark (?) next to the container that contains the connectors in the left panel. Refer to "Resolving Invalid Certificate Errors" on page 125.

Adding Locations and Hosts from a File

To add hosts (and consequently, containers and connectors) in bulk, you can use a comma-separated values (CSV) file. 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 credentials. When the certificates are retrieved, you are prompted to import them.

Note

A host is **not** added if:

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

The CSV file needs to be in the format shown in the following example. Also, ensure that an end-of-line character is included in the last line of the CSV file if the file was created on a Windows system. However, an end-of-line character is not required if the file was created on a Linux system.

	A	B	C	D	E	F
1	**Location**	**Hostname**	**Port**	**Type**	**User**	**Password**
2	East	ernie.company.com	9006	8 Containers	admin	password
3	West	elmo.company.com	9008	Software	admin	password
4						

To add locations and hosts from a CSV file:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel.
3. Click (on top of the page) in the right panel to open the wizard.

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

5 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 your mouse over the certificate.)

- Select **Import the certificates to Connector Appliance from the containers**, then click **Next** to import the certificates and continue.
- Select **Do not import the certificates to Connector Appliance from the containers** and 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.

Editing a Location

You can edit the name of a location from the System-level page or from a specific Location page.

To edit a location:

1 Click **Manage** from the top-level menu bar.

2 From the System-level page:

Click **System** (left panel) > **Locations** tab (right panel) >  in the Action column.

From a specific Location page:

Click **System** (left panel) > *Location* >  (on top of the page, in the right panel).

3 Enter the new name of the location and click **Next**.

4 Click **Done**.

Deleting a Location

When you delete a location, the hosts, containers, and connectors that it contains are also deleted.

To delete a location:

1 Click **Manage** from the top-level menu bar.

2 Click **System** in the left panel.

3 Select the location you want to delete. You can select multiple locations.

4 Click **Delete** at the bottom of the page, in the right panel.

Adding Hosts to a Location

See "Adding a Host" on page 106.

Hosts

A host is a computer on a network, associated with an IP address, on which connectors are installed. A host can be of three types:

- The Localhost (the local Connector Appliance or the Logger appliance running Connector Manager). By default, **Localhost** exists on a brand new Connector Appliance or Logger appliance running Connector Manager; it contains a default number of containers, which are empty.
- A remotely-managed Connector Appliance.
- A Software-type host (a Windows, Linux, or UNIX system running software-based connectors from ArcSight). A software-type host can contain up to 20 containers.

You can view all hosts on the system, and view containers and connectors in a host. You can add, scan, delete, and edit a host. You can move a host to a different location and upgrade a host remotely. You can also add a container to a host. All these procedures are described below.

Viewing All Hosts

You can see all the hosts you are managing.

To view all hosts:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left pane. All hosts display on the Hosts tab in the right panel.

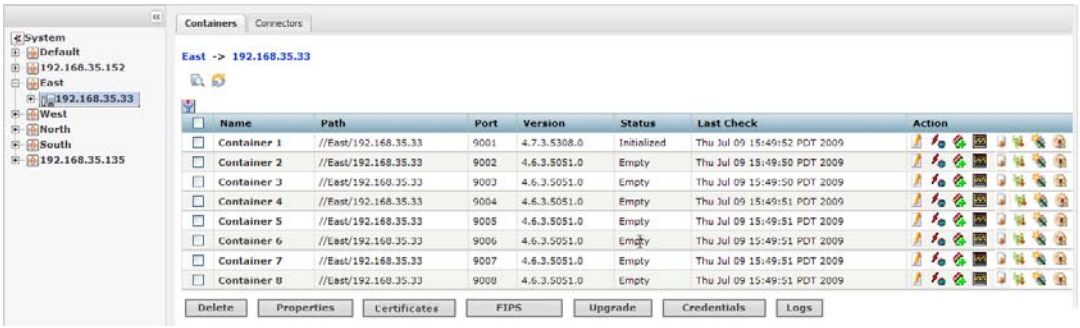
Viewing Containers and Connectors in a Host

You can see all the containers and connectors that exist on a host.

To view containers and connectors on a host:

1. Click **Manage** from the top-level menu bar.
2. In the left panel, click the location (under System) in which the host exists.
3. In the left panel, click the host to view the containers and connectors.

   All containers display on the Containers tab and all connectors display on the Connectors tab in the right panel.



Adding a Host

By default, a local host **Localhost** exists on your Connector Appliance or Logger appliance running Connector Manager. However, Connector Appliance can manage connectors installed on other Connector Appliances and other systems such as Windows, UNIX, or Linux. To manage remote connectors, you need to add the hosts on which those connectors are running.

When you add a host, the system also attempts to retrieve the CA certificates from the containers that reside on the host. Containers on the remote host can be managed only if the system can authenticate using the certificates and the credentials. When the certificates are retrieved, you are prompted to import them.

A host is **not** added if:

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

You can add hosts from the System-level page or from a specific Location page.

You can also add locations and hosts using a comma-separated values (CSV) file. For more information see, "Adding Locations and Hosts from a File" on page 103.

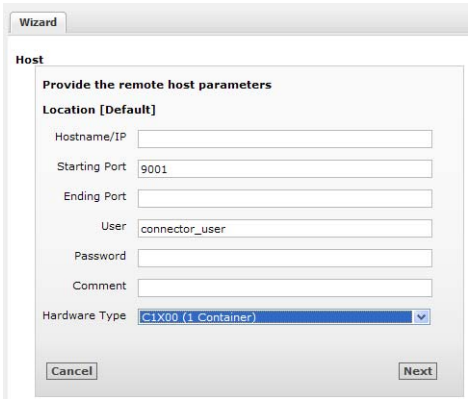
When you add a remote software-type host, it is scanned automatically for the currently-running containers and the connectors associated with them. If additional containers are added to the remote host after it has been added to the system, you need to scan the host manually to detect the new containers. For information about scanning hosts, see "Scanning a Host" on page 108.

To add a host:

1. Click **Manage** from the top-level menu bar.
2. From the System-level page, click **System** (left panel) > **Locations** tab (right panel) >  in the Action column.

   From a specific Location page, click **System** (left panel) > *Location* (under which the host exists) >  (on top of the page, in the right panel).

3 On the Host Wizard form, shown below, enter values for the parameters listed in the following table and then click **Next**



Parameter	Description
Hostname	The hostname or IP address of the actual host.
Starting Port	Each container on a host listens on a port. Specify the starting port number. Subsequent containers will use subsequent ports.
User	The user name that the system uses to connect to the host.
Ending Port	By default, Connector Appliance scans port 9001 to port 9020 when adding a host. If you select **software** in the **Hardware Type** field, you can specify the ending port number (for example, 9003) to speed up the add host process.
Password	The password for the user name you specify.
Comment	A meaningful description for the host you are adding.
Hardware Type	• If you want to manage connectors that reside on a remote Connector Appliance, select the number of containers on that host. A host can have up to 8 containers. For the number of connectors applicable to each model type and container specifics, see the *ArcSight Appliance Specifications* document. This document is available on the ArcSight Customer Support site at http://www.arcsight.com/supportportal. • If you want to remotely manage connectors running on a Windows, UNIX, or Linux system, select **Software**. The system can detect the presence of software-based connectors on remote hosts using the Starting Port value you specified earlier. The system scans up to 20 configurable ports from the starting port to find the "listening" connectors. Any found connectors are added into the host. For more information, see "Scanning a Host" on page 108.

4 Connector certificates are retrieved automatically so that the system can communicate with each connector in a container. The Add Host wizard lists the certificates. (To see certificate details, hover your mouse over the certificate.)

- Select **Import the certificates to Connector Appliance from the containers**, then click **Next** to import the certificates and add the host.

- Select **Do not import the certificates to Connector Appliance from the containers** and click **Next** if you do not want to import the certificates. Connector Appliance does not add the host.

Note

The Add Host wizard does not add the host if the certificate download failed for any of the connectors in a container or if any of the certificates failed to import into the trust store.

Scanning a Host

Scanning a host enables the system to detect new or removed containers from a remote ***software-type*** host. When a software-type host is added for the first time, it is scanned automatically for containers running at that time; however, to keep this information up-to-date, you need to scan the host manually whenever you add connectors to the remote host.

You can scan a host from the System-level page, a specific Location page, or a specific Host page.

Note

- You can scan only software-type hosts. See "Hosts" on page 105 for information about software-type hosts.
- The connectors on a software-type host need to be configured for remote management.
- A maximum of 20 connectors are scanned on port 9001 through 9020.

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 the system can authenticate using the certificates and the credentials. When the certificates are retrieved, you are prompted to import them.

Note

A host cannot be scanned (the scan fails) if:

- Any containers on the 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 **Manage** from the top-level menu bar.
2. From the System-level page, click **System** (left panel) > **Locations** tab (right panel).

   From a specific Location page, click **System** (left panel) > *Location* (under which the host exists).

   From a specific Host page, click **System** (left panel) > *Location* (under which the host exists) > *Host*.
3. Click  in the Action column for the host that you want to scan.
4. Click **Next** in the Host Scan wizard.

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

Parameter	Description
Starting Port	The port number on the host on which Connector Appliance starts scanning for containers.
Ending Port	The port number on the host on which Connector Appliance ends scanning for containers.
User	The user name that the system uses to authenticate with the host.
Password	The password for the user name you provide.

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

- Select **Import the certificates to Connector Appliance from the containers**, then click **Next** to import the certificates and continue.
- Select **Do not import the certificates to Connector Appliance from the containers** and click **Next** if you do not want to import the certificates. The Host Scan wizard does not continue the scan.

The scan is not completed if the certificate download failed for any of the connectors in a container or if any of the certificates failed to import into the trust store.

Deleting a Host

When you delete a host, the containers and connectors that it contains are also deleted from the system that is managing the host. You can delete a host from the System-level page or from a specific Location page.

To delete a host:

1 Click **Manage** from the top-level menu bar.

2 From the System-level page, click **System** (left panel) > **Hosts** tab (right panel).

From a specific Location page, click **System** (left panel) > *Location* (under which the host exists).

3 Select the host you want to delete. You can select multiple hosts.

4 Click **Delete** on the bottom of the page.

Moving a Host to a Different Location

When you move a host, the containers and connectors that it contains are also moved. You can move a host from the System-level page or from a specific Location page.

To move a host:

1. Click **Manage** from the top-level menu bar.
2. From the System-level page, click **System** (left panel) > **Hosts** tab (right panel).

   From a specific Location page, click **System** (left panel) > *Location* (under which the host exists).
3. Select the host you want to move. You can select multiple hosts.
4. Click **Move** at the bottom of the page.
5. Follow the instructions in the Hosts Move wizard.

Editing a Host

You cannot edit a host, however, you can delete an existing host and add a new one (as described in "Adding Hosts to a Location" on page 104) or move an existing host (as described in "Moving a Host to a Different Location" on page 110).

Upgrading a Host Remotely

If you are upgrading the local host, refer to the instructions in the Release Notes for this release. The following instructions only apply to upgrading a remotely-managed Connector Appliance.

You can upgrade a single remotely-managed Connector Appliance or several remotely-managed Connector Appliances at the same time (in bulk). Follow these guidelines:

- You need to upgrade at least one Connector Appliance to version 5.5 by following instructions in the Connector Appliance v5.5 Release Notes before using this feature to upgrade other appliances in your network.
- The containers of the appliance being upgraded need to be managed on the Connector Appliance from which you will initiate the upgrade.

The following table compares a local host upgrade (System Update) to a remote Connector Appliance upgrade (Remote Upgrade).

Remote Upgrade	System Update
Can upgrade more than one host at a time.	Can only upgrade the local host
The upgrade is performed by pushing the `.aup` file to the remote Connector Appliance.	The upgrade is performed by applying the `.enc` file on the local host.

Remotely upgrading a Connector Appliance is a two-step process.

To upgrade a Connector Appliance remotely:

1. Upload a Connector Appliance .aup upgrade file from the ArcSight Customer Support site to the Upgrade AUP repository.

   This step is only required if the version that you want to upgrade does not already exist in the repository.

2. Push the `.aup` upgrade file to the remote Connector Appliances, as follows:

   a. Click **Manage** from the top-level menu bar.

   b. From the System-level page, click **System** (left panel) > **Hosts** tab (right panel).

      From a specific Location page, click **System** (left panel) > *Location* (under which the host exists).

   c. Select the host you want to upgrade. You can select multiple hosts.

   d. Click **Upgrade** at the bottom of the page.

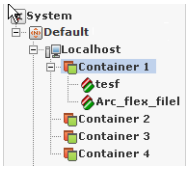
   e. Follow the instructions in the upgrade wizard.

Adding a Container to a Host

See "Adding a Container" on page 113.

Containers

A container is a single Java Virtual Machine (JVM) that can run up to four connectors. The following illustration depicts Container 1 and the connectors it runs.



A default number of containers exist on each Connector Appliance. The number depends on the Connector Appliance hardware platform. Each container is identified with a label (Container Name) and an associated port number (9001 or higher).

Connector Manager on a Logger appliance contains one default container in the default host **Localhost**. You cannot delete this container.

You can perform many operations on containers. You can view all containers on the system and view the connectors in a container. You can add, delete, and edit a container. You can update container properties and change container credentials. You can manage certificates on a container, run a command on a container, and upgrade a container to a specific connector version. You can also view and delete container logs and run the Logfu utility. All these procedures are described below.

If you see a question mark (?) next to a container in the left panel, as shown below, 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 125.

Viewing All Containers

You can see all the containers you are managing.

To view all containers:

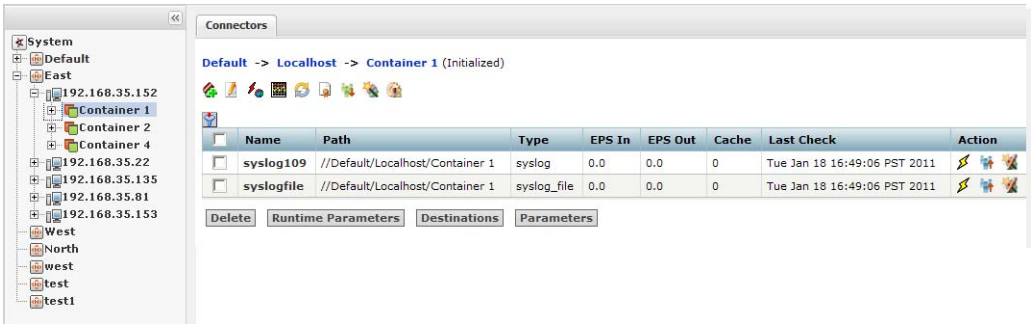
1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel. All containers display on the Containers tab in the right panel.

Viewing Connectors in a Container

You can see all the connectors in a container.

To view connectors in a container:

1. Click **Manage** from the top-level menu bar.
2. In the left panel, click the *Location* > *Host* (under which the container exists) > *Container* (whose connectors you want to view). The connectors are listed on the right panel.



Adding a Container

You do not need to add a container as containers are added automatically when a new host is added to the system.

When you add a software-type host, it is scanned automatically for containers (and connectors) as described in "Scanning a Host" on page 108. If you add connectors to such a host at a later date, you need to scan it manually.

Adding a Connector to a Container

See "Adding a Connector" on page 130.

Editing a Container

The default names for containers are numerical, but you can change them.

To edit a container:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click System (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

User Interface Options	Path
From the Containers page	Click System (left panel) > *Location* (left panel) > *Host* (left panel).

3 Click  in the Action column of the container whose name you want to change.

If you are on the specific Container page,  is at the top of the page.

4 Enter the new name in the **Name** field and click **Next**.

5 Click **Done**.

Deleting a Container

You can delete containers from ***software-type*** hosts only. All other hosts (for example, a remotely-managed Connector Appliance) have a fixed number of containers.

When you delete a container, the connectors that it contains are also deleted.

To delete a container:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3 Select the container you want to delete. You can select multiple containers.

4 Click **Delete**.

Updating Container Properties

You can update existing container properties (located in the `agent.properties` file), delete them, or add new ones.

To update container properties:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).

User Interface Options	Path
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

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.

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`. For security reasons, it is important to change these values before deploying the system in production.

To change container credentials:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3 Select the container whose credentials you want to update. You can select multiple containers.

4 Click **Credentials**.

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

This feature does not apply for containers managed by another Connector Appliance, as that appliance will not be notified of the changes. If the local system tries to communicate with the remote Connector Appliance, a credentials error occurs.

Enabling and Disabling FIPS on a Container

You can enable or disable FIPS mode on a container. When FIPS mode is enabled for a container, all the connectors in that container are in FIPS mode.

FIPS mode is supported on local, remote, and software connectors running version 4.7.5 or later. Certain connectors do not support FIPS mode. For information about which connectors do not support FIPS mode, contact ArcSight Customer Support.

Note

Before enabling FIPS on a container that contains software connectors running as a service, review the caveats listed in document *Installing FIPS-Compliant SmartConnectors*, available from ArcSight Customer Support.

Note

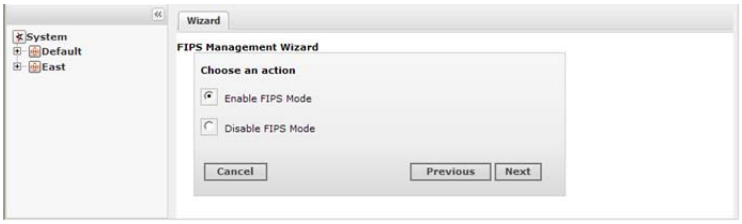
After you enable or disable FIPS mode on a container, check that the appropriate CA certificates are in the trust store of the connectors so that they can validate their configured destinations successfully. If the appropriate CA certificates are not present, you need to add them (refer to "Managing Certificates on a Container" on page 117).

To enable or disable FIPS mode on a container:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3. Select the container on which you want to enable or disable FIPS mode. You can select multiple containers.
4. Click **FIPS**, then click **Next** to run the FIPS Management wizard.



5. Click **Enable FIPS Mode** or **Disable FIPS Mode**, then click **Next**.

If FIPS mode is already enabled or disabled on the container, the FIPS Management wizard indicates this on the Summary page.

6 Check that the appropriate CA certificates are in the trust store so that the connectors in the container can validate their configured destinations successfully. If necessary, add the appropriate certificates to the container. Refer to Managing Certificates on a Container.

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:

- Enable or disable a demo certificate on a container.
  You can enable a demo certificate on a container that is in non-FIPS mode only.
- Add a certificate on a container.
- Add a CA Certs file on a container.
  You can 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 123.

For information about resolving invalid certificates, see “Resolving Invalid Certificate Errors” on page 125.

Adding CA Certificates on a Container

You can add a single CA certificate on 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 your mouse 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 follow the following procedure, make sure that the certificate you want to apply is loaded in the CA Certs repository.

To apply a single CA certificate on a container:

1 Click **Manage** from the top-level menu bar.

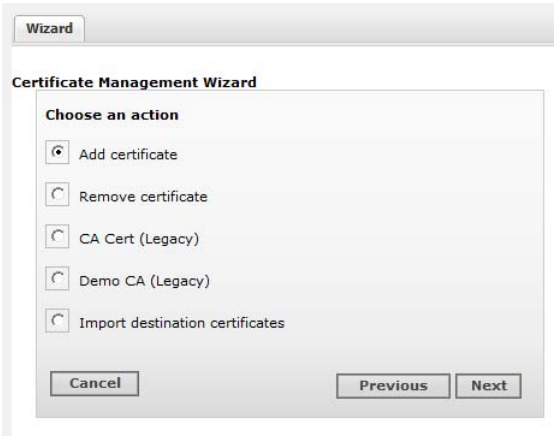
2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3 Select the container to which you want to add the certificate. You can select multiple containers.

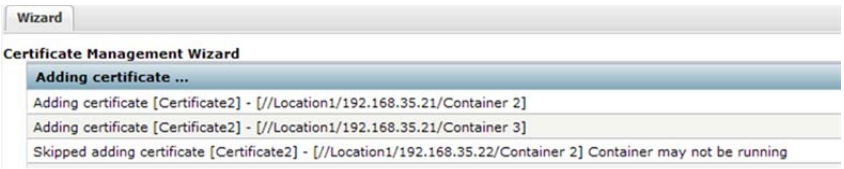
4 Click **Certificates**, then click **Next** to run the Certificate Management wizard.

5 Click **Add Certificate** to add a certificate.



6 Follow the instructions in the wizard.

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.

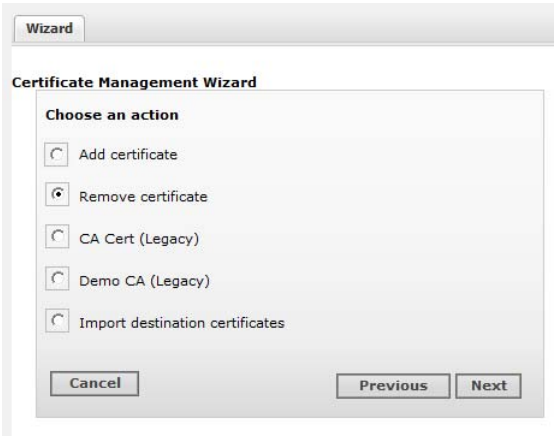
Use caution when deleting certificates. When you delete a certificate on a container but the connector destination is still using that certificate, the connector can no longer communicate with the destination.

To remove CA certificates from a container:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

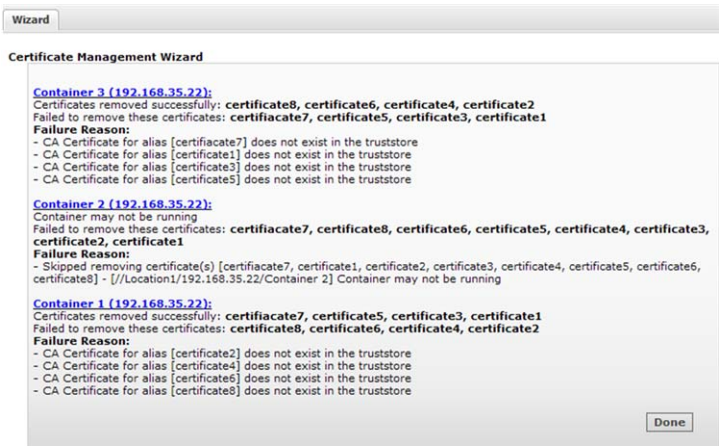
3. Select the container from which you want to remove the CA certificates. You can select multiple containers.
4. Click **Certificate**, then click **Next** to run the wizard.
5. Click **Remove certificate** and click **Next**.



6. Select one or more certificates from the certificate list and 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.

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 on a Container

You can add a CA Certs file on 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.

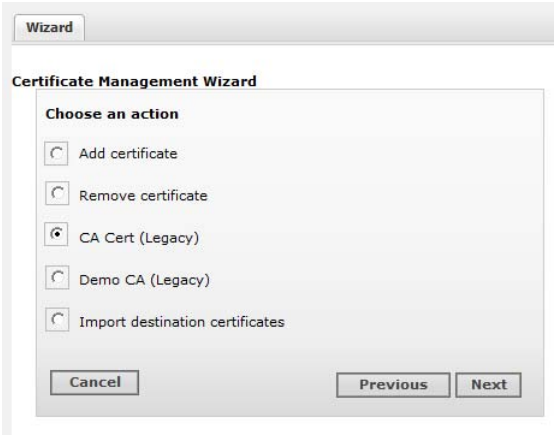
To add a CA Certs file on a container:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3. Select the container to which you want to add the CA Certs file. You can select multiple containers.
4. Click **Certificates**, then click **Next** to run the wizard.

5 Click **CA Cert (Legacy)**. You can add a CA Certs file to a container only if it is in non-FIPS mode.



6 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.

Note

- 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.
- Hover your mouse over a container name to see the type of certificate applied to it.

To enable or disable a demo certificate on a container:

1 Click **Manage** from the top-level menu bar.

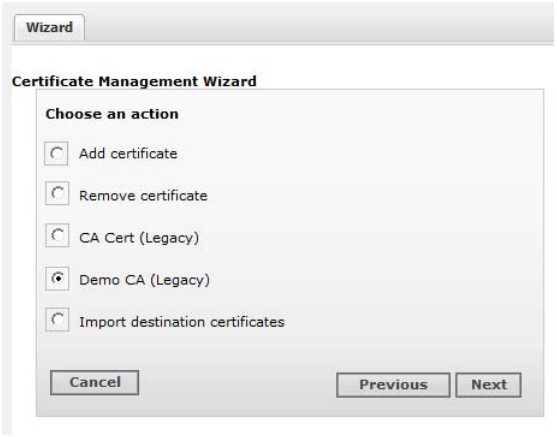
2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3 Select the container to which you want to apply the demo certificate. You can select multiple containers. All the containers need to be in non-FIPS mode.

4 Click **Certificates**, then click **Next** to run the Certificate Management wizard.

5 Click **Demo CA (Legacy)**, then click **Next**.



6 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.

Note

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 **Manage** from the top-level menu bar.

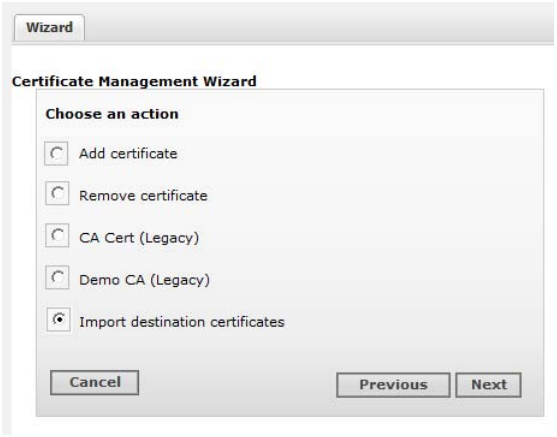
2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3 Select the container to which you want to add the certificates. You can select multiple containers.

4 Click **Certificates**, then click **Next** to run the Certificate Management wizard.

5 Click **Import destination certificates** to add a certificate.

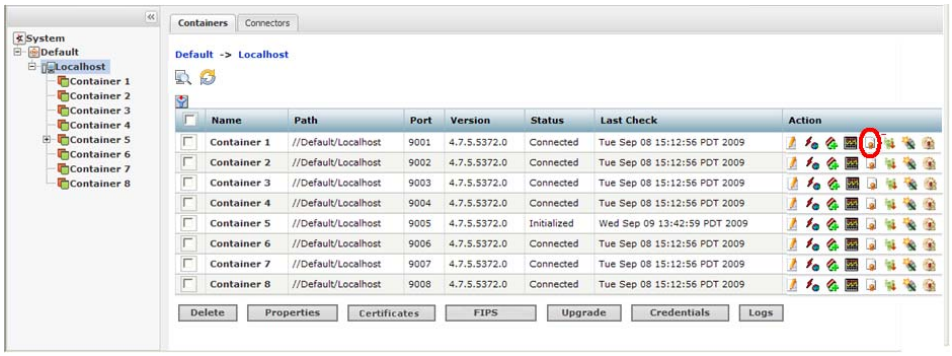


6 Follow the instructions in the wizard.

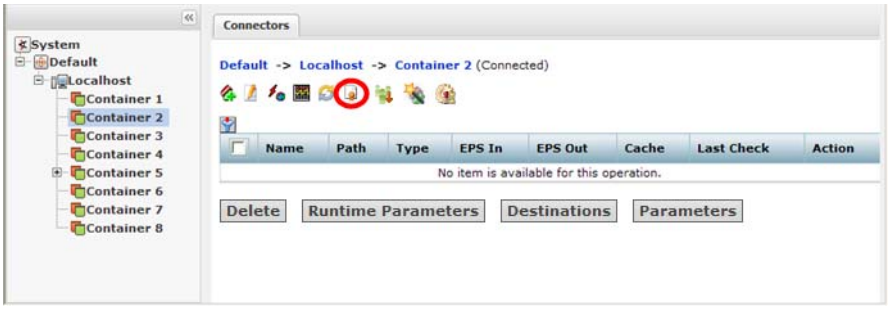
Viewing Certificates on a Container

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 click **Next** at the bottom of the page.

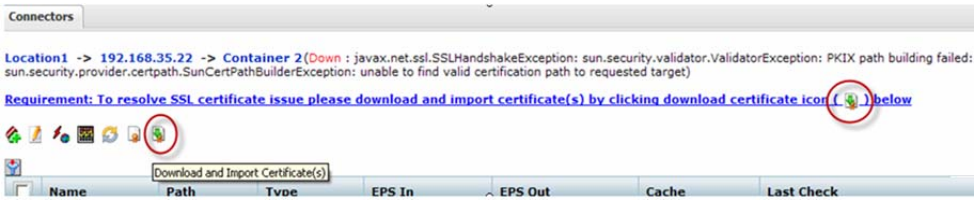
Resolving Invalid Certificate Errors

If no valid CA certificates exist for the connectors in the container, you see a question mark (?) next to the container in the left panel, as shown below.

To resolve the invalid certificate error:

1 Click the container name in the left pane to view the certificate error on the Connectors tab.

2 Click the  icon to run the Certificate Download wizard.



3 Follow the instructions in the wizard to import the valid certificates.

Running a Command on a Container

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

To run a command on a container:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).
From the Container page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Container**.

3 Click  in the Action column of the container.

If you are on the specific Container page,  is at the top of the page.

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

5 Enter values for the parameters that the user interface displays and click **Done**.

Upgrading a Container to a Specific Connector Version

All connectors in a container are upgraded to the version you select.

You can't upgrade the same container more than once within a short period of time. After you upgrade a container, wait at least 15 minutes before upgrading it again.

To upgrade a container to a specific connector version:

1 Upload a connector build AUP from the ArcSight Customer Support site to the AUP (Upgrade) repository.

This step is only required if the build does not already exist in the AUP (Upgrade) repository.

2 Apply the connector build to a container, as follows:

a Click **Manage** from the top-level menu bar.

b Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > Location (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > Location (left panel) > **Host** (left panel) > **Containers** tab (right panel).

c Select the container that you want to upgrade. You can select multiple containers for a bulk upgrade.

d Click **Upgrade**.

e Select the version to which you want to upgrade the selected containers and 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, you can upload the `.aup` file to a higher-performance system if one is available, then push the result to the lower-performance system.
- If you are upgrading an empty container, the system creates a temporary connector during the upgrade process. You can safely ignore this temporary connector; it is deleted shortly after being created.
- Empty connectors can be upgraded from versions **5.1.2 and after**. Upgrading empty connectors is not supported in previous versions.

Viewing Container Logs

You can retrieve and view the log files for a container. The log files are in `.zip` format.

To view container logs:

1 Load the logs to the Logs repository.

If the logs that you want to view are already in the Logs repository, skip this step.

a Click **Manage** from the top-level menu bar.

b Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

c Select the container whose logs you want to view. You can select multiple containers.

d Click **Logs**.

The logs are loaded to the Logs repository. If you selected multiple containers, a log file for each container is loaded.

2 Retrieve and view the logs:

a Click **Setup** > **Repositories** from the top-level menu bar.

b Click **Logs**.

c Click  to retrieve the log files (in `.zip` format) you want to view.

Deleting Container Logs

To delete a container log file, click **Setup** > **Repositories** > **Logs** >from the top-level menu bar. In the right panel, click next to the log files you want to delete.

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 (with a connector or the connected device), it is useful to have a visual representation of what happened over time. You can use Logfu to analyze this behavior.

To run Logfu on a container:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).
From the Container page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3. Click  in the Action column of the container. A separate window is displayed. If you are on the specific Container page,  is at the top of the page.

   The system proceeds to retrieve and analyze system data logs. After this process is complete, a group of panels appear in the window.
4. From 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 and logs.

   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.
5. 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.
6. If you need to choose a different data point for analysis, click **Reset Data**.

Running Diagnostics on a Container

You can run certain diagnostics on a local or remote container. Currently, the **Edit a File** diagnostic action only is available:

The **Setup** > **System Admin** tab also provides diagnostic tools, which you can run on the local appliance only; refer to "Diagnostic Tools" on page 35.

To run diagnostics on a container:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).
From the Container page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel). The **Connectors** tab displays.

3 To open the Container Diagnostics wizard:

- From the **Container** tab, click in the **Action** column.
- From the **Connectors** tab, click  at the top of the page.

4 Follow the steps in the wizard:

a 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.

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

On Mozilla Firefox, if the text is underlined with red lines, right click on the text area and uncheck **Check Spelling**.

When you click **Next**, Connector Appliance saves the updated file in the `user/agent` folder on the container; the original file is overwritten.

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

Connectors

A connector (also known as a SmartConnector) is an ArcSight software component that collects events and logs from various sources on your network. A connector can be configured on a Logger appliance running Connector Manager, on a Connector Appliance, or can be installed on a computer on your network and managed remotely. For a complete list of supported connectors, go to the 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, and run the Logfu utility. All these procedures are described below.

Whenever applicable, the above listed operations can be performed on more than one connector at a time. Each procedure described in this section indicates if multiple connectors can be selected when performing a procedure.

Viewing all Connectors

You can see all the connectors you are managing.

To view all connectors:

1. Click **Manage** from the top-level menu bar.
2. Click **System** in the left panel. The connectors display on the Connectors tab in the right panel.

Adding a Connector

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 using procedures described in "Adding a Location" on page 102, "Adding a Host" on page 106, and "Adding a Container" on page 113.
- Follow the configuration best practices described in "Configuration Suggestions for Connector Types" on page 164.

  If you are configuring the Check Point OPSEC NG Connector, see "Configuring the Check Point OPSEC NG Connector" on page 165 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 168.

This connector type has special requirements concerning JDBC and authentication setup. It is important that you 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 115.

- 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, a CIFS share needs to be configured before you add those connectors. For information on creating a CIFS Mount, see "Remote File Systems" on page 44.

  For all other connectors, an NFS Mount needs to be established before the connector can be added. For information on creating an NFS Mount, see "Remote File Systems" on page 44.

- 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.

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 165.

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).
From the Container page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Click  in the Action column of the container to run the wizard to configure a connector.

If you are on the specific Container page,  is at the top of the page.

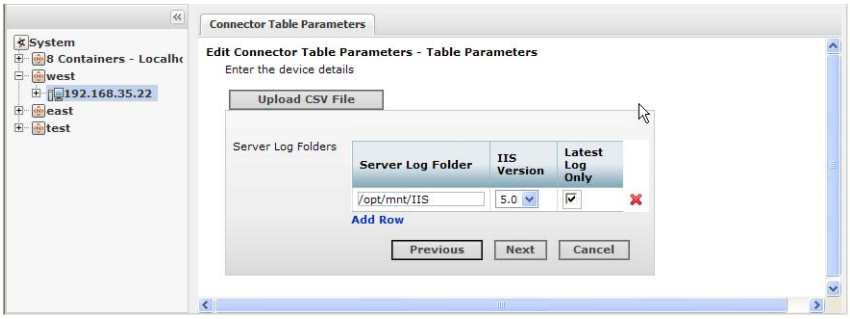
4 Select a connector type from the pull-down list of available types. Click **Next**.

5 Enter basic parameters for the connector. Parameters vary based on the connector type. You can hover the mouse pointer over a field for more information. When all fields have been entered, click **Next**.

Note

When entering parameters that include a file path, enter the path in POSTIX format (for example, `/folder/filename`). If you enter the path in DOS/NTFS format (for example, `\folder\filename`), the backslash (`\`) is included as part of the file name and the path will be incorrect.

For file-based connectors on Windows systems, specify the name of the CIFS mount point you created for the connector, as shown in the following example. (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. See "Adding Locations and Hosts from a File" on page 103 for the file format. 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.

Note

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, Connector Appliance 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.

Note

For detailed information about individual connector parameters, refer to the specific *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.

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

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

For containers running v5.1.2.5823 and later, Connector Appliance retrieves the certificate for the destination automatically and displays the certificate summary. To see certificate details, hover your mouse over the certificate.

- Select **Import the certificate to the connector from the destination**, 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.

For containers running v5.1.2 and earlier, upload the certificate on the container and then add the destination.

Note: FIPS Suite B mode is not supported. Connector Appliance cannot download a manager certificate in Suite B mode.

7 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.
Comment	Additional comments.

Configuring a connector can take some time; the connector might initially display *Down* while it is restarting.

8 Click **Done**.

Editing Connector Parameters

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 at the same time.

Updating Simple Parameters for a Specific Connector

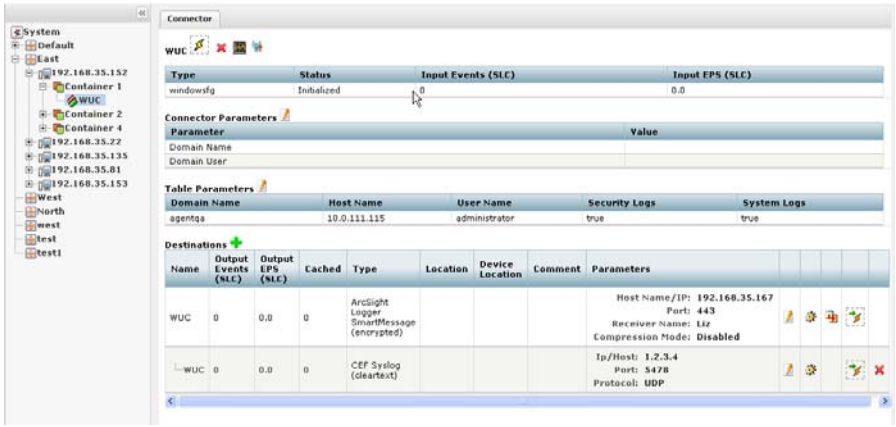
The following procedure describes how to update simple parameters for a specific connector. To update *table* parameters for a specific connector, see "Updating Table Parameters for a Specific Connector" on page 136. To update both simple and table parameters for multiple connectors at the same time, see "Updating Simple and Table Parameters for Multiple Connectors" on page 137.

To update parameters for a specific connector:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) next to the **Connector Parameters** link.



Note

Clicking the heading **Connector Parameters** toggles between displaying and hiding the information in the Connector Parameters section.

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

Note

- Configuration parameters depend on the type of connector being configured.
- When editing parameters that include a file path, enter the path in POSTIX format (for example, `/folder/filename`). If you enter the path in DOS/NTFS format (for example, `\folder\filename`), the backslash (`\`) is included as part of the file name and the path will be incorrect.

5 Click **Done** when complete.

The updated parameters display in the Connector Parameters section of the Connector page.

Updating Table Parameters for a Specific 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 **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) next to the **Table Parameters** link.

Note: Clicking the heading **Table Parameters** toggles between displaying and hiding the information in the Table Parameters section.

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.

- To export the table parameters to a CSV file for use as a backup or to import on another Connector Appliance, click the **Export File** button.

5 Click **Done** when complete.

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 at once:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Select the connectors whose parameters you want to update.

The connectors must be the same type; for example, you can change the parameters for several syslog connectors at the same time; however, you cannot change the parameters for several syslog and several SNMP connectors at the same time.

4 Click **Parameters**.

5 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 3 on page 136). 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 that are of different versions, the newer connectors might have additional parameters. In this case, only the parameters that are the same for all connectors are displayed for updating.

Managing Destinations

Connectors can forward events to more than one destination, such as ArcSight ESM 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

- You cannot configure two connectors with the same ESM Manager destination if the destination (connector) name and location used for configuration is the same.
- Logger receivers do not support encrypted data.
- You cannot use the **Edit** button ( ) to change or add a connector destination. Its purpose is to change destination parameters. To add a new destination, remove the unwanted destination configuration ( ) and create a new one ( ).

Adding a Primary Destination to a Specific 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.

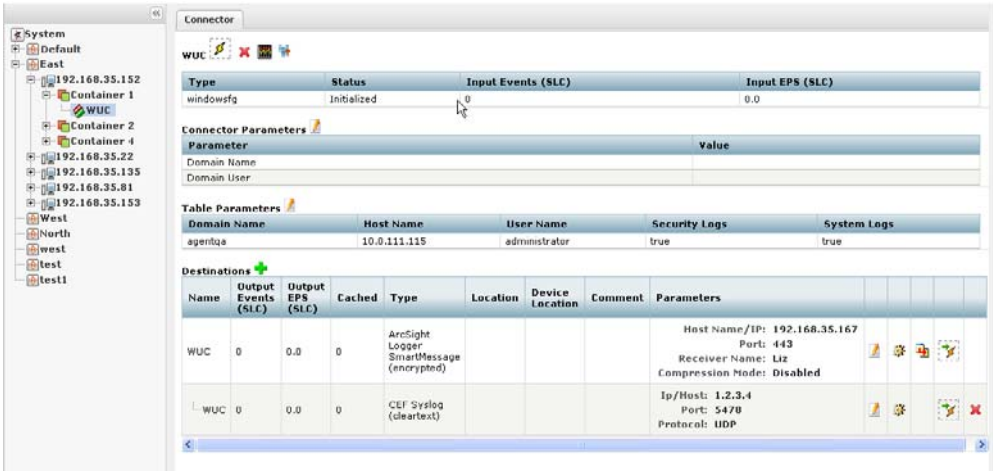
To add a primary destination to a connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) next to the **Destinations** link.



Note

Clicking the **Destinations** heading toggles between displaying and hiding the information in the Destinations section.

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 v5.1.2.5823 and later, Connector Appliance retrieves the certificate for the destination automatically and displays the certificate summary. To see certificate details, hover your mouse over the certificate.

- Select **Import the certificate to the connector from the destination**, 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.

For containers running v5.1.2 and earlier, upload the certificate on the container and then add the destination.

Note: FIPS Suite B mode is not supported. Connector Appliance cannot download a manager certificate in Suite B mode.

5 Click **Done** when complete.

Adding a Failover Destination to a Specific 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:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) in the Destinations section to display the Add Connector Destination wizard.

4 Follow the steps in the wizard to select from available destinations and enter the destination details.

For containers running v5.1.2.5823 and later, Connector Appliance retrieves the certificate for the destination automatically and displays the certificate summary. To see certificate details, hover your mouse over the certificate.

- Select **Import the certificate to the connector from the destination**, 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.

For containers running v5.1.2 and earlier, upload the certificate on the container and then add the destination.

Note: FIPS Suite B mode is not supported. Connector Appliance cannot download a manager certificate in Suite B mode.

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 more than one connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Select all connectors to which you want to assign a destination.

4 Click **Destinations** at the bottom of the page to open the wizard.

5 Select **Add a destination** and click **Next**.

6 Choose between a creating a new destination or selecting an existing destination, 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.

Connector Appliance retrieves the certificate for the destination automatically and displays the certificate summary. To see certificate details, hover your mouse over the certificate.

- Select **Import the certificate to the connector from destination**, 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.

Note: FIPS Suite B mode is not supported. Connector Appliance cannot download a manager certificate in Suite B mode.

7 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**:

a Select the primary destination that applies to your failover.

b Click the check box in the table header to modify all of the displayed connectors.

c Click **Next** to update the configuration.

8 Click **Done** when complete.

Removing Destinations

You can remove a destination from a connector at any time. The following procedures describe how to remove a single destination from a specific connector and how to remove multiple destinations from one or more connector.

To remove a single destination from a *specific* connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 In the Destinations section, click  for the destination you want to remove.

The  shows in the Destinations table only if more than one destination is listed.

4 When prompted, confirm the removal.

To remove *multiple* destinations from one or more connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).

User Interface Options	Path
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Select the connectors whose destinations you want to remove.

4 Click the **Destinations** button to open the wizard.

5 Select **Remove destinations** and click **Next**.

6 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 connector; for example, after you upgrade ESM, or if a Logger appliance or ESM appliance becomes unresponsive.

To re-register destinations for one or more connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Select the connectors whose destinations you want to re-register.

4 Click the **Destinations** button to open the wizard.

5 Select **Re-register destinations** and click **Next**.

6 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 at the same time.

You cannot change the connector type; however, you can remove the unwanted connector configuration and create a new one.

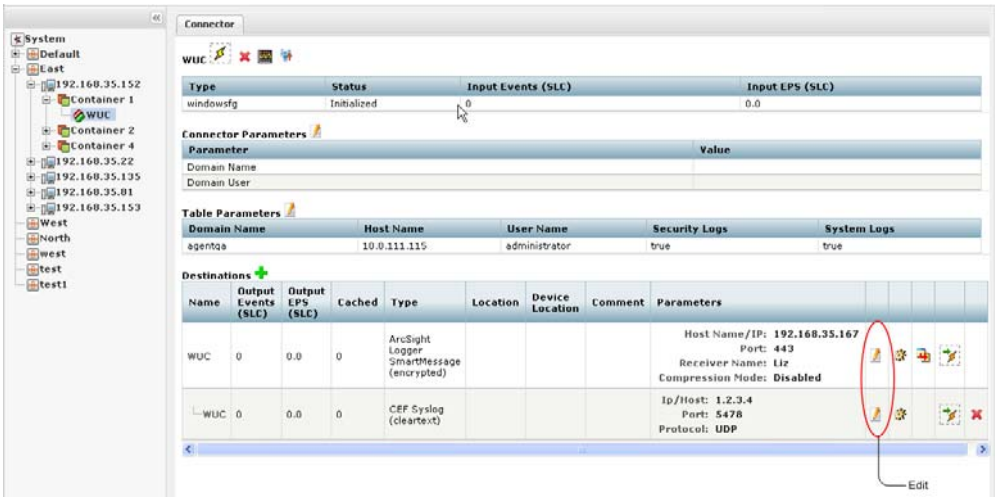
To edit destination parameters for a *specific* connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 In the Destinations section, click ( ) next to the destination you want to edit to display the Edit Destination Parameters page.



Caution

You cannot use the **Edit** button ( ) to change or add a connector destination. Its purpose is to change destination parameters. To add a new destination, remove the unwanted destination ( ) and create a new one ( ).

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

5 Click **Done** when complete.

To edit destination parameters for *multiple* connectors:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3 Select the connectors whose destination parameters you want to edit.

4 Click **Destinations** to open the wizard.

5 Select **Edit a destination** and click **Next**.

6 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 parameters you can configure are listed in Appendix C, Destination Runtime Parameters, on page 189. All the parameters listed in that table are not available for all destinations. 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 specific* connector:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3. In the Destinations section, click  next to the destination whose runtime parameters you want to edit.
4. 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 149.
5. Specify or update values for the listed parameters and click **Save**.

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

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).
From the Connectors page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* (left panel).

3. Select the connectors whose destination runtime parameters you want to edit.
4. Click **Runtime Parameters** to open the wizard.
5. 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

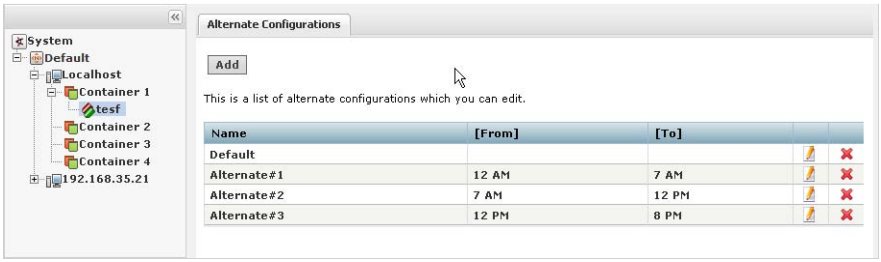
An alternate configuration is a set of runtime parameters that is used instead of the default configuration during a specified portion of every day. For example, you might want to specify different batching schemes (by severity or size) for different times of a day. You can define more than one alternate 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 am to 5 pm time range and another configuration for the 5 pm to 8 am time range.

By default, a configuration labeled **Default** exists and 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 am to 8 pm, the **Default** configuration will be used from 8 pm to 7 am (assuming that there are no other alternate configurations defined on this system).

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 **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).

User Interface Options	Path
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) in the Destinations section.

4 Click **Add**.

5 Specify or update values for the listed parameters.

6 Scroll down to the end of the page and 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 **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click ( ) in the Destinations section.

4 Select the alternate configuration that you want to edit and 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**.

Specifying a Time Range for an Alternate Configuration

See "Editing an Alternate Configuration" on page 150.

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 147.

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 **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3. Click () in the Destinations section.
4. Select the command you want to run and click **Next**.
5. Enter values for the parameters that the user interface displays and click **Finish**.

Removing a Connector

After removing a connector, you need to reboot the system; otherwise, the removed connector continues to forward events to its destination.

To remove a Connector:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel).

3. Select the connectors you want to delete. You can select multiple connectors.
4. Click **Delete** at the bottom of the page.
5. Reboot the system.

You can also delete a specific connector from its details page: Click **System** (left panel) > **Location** (left panel) > **Host** (left panel) > **Container** > **Connector** > at the top of the page.

Sending a Command to a Connector

You can send a command to a connector.

To send a command to a connector:

1 Click **Manage** from the top-level menu bar.

2 Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3 Click  in the Action column for the connector.

If you are on a specific Connector page,  is on top of the page.

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

5 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 run Logfu on a connector:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3. Click () on top of the page. A separate window displays.

   The system proceeds to retrieve and analyze system data logs. After this process is complete, a group of panels appears in the window.
4. From 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 and logs.

   Choose one of the Group box **data points**. Depending on which data point you choose, a list of fields appears in the Field box below.
5. 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.
6. If you need to choose a different data point for analysis, click **Reset Data**.

Changing the Network Interface Address for Events

Connector Appliance has multiple network interfaces. By default, the connector determines which network interface address is used for events displayed in the ESM 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.

Connector Appliance 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 ArcSight Customer Support site).

Currently, 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 ArcSight SmartConnector.

To develop a FlexConnector:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths to go to the **Containers** tab:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3. Click  in the Action column of the container to which you want to add the FlexConnector. When the FlexConnector Development wizard opens, click **Next**.
4. Provide the vendor and product name of the device for which you are creating a FlexConnector, then click **Next**.

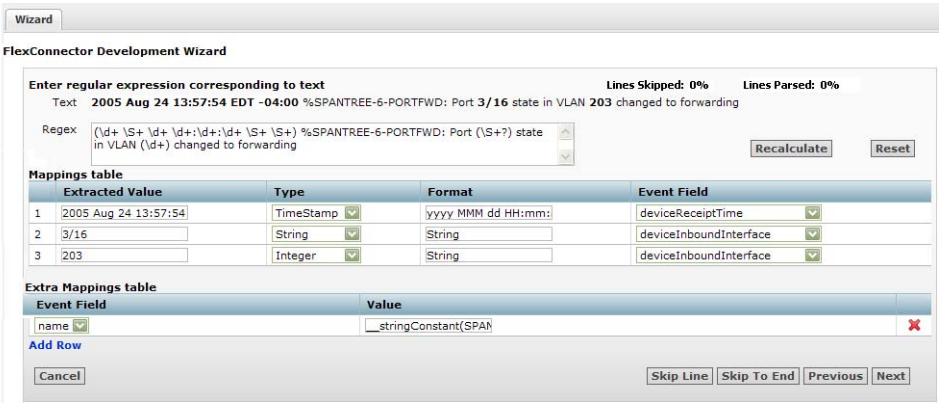
The device vendor and product name are required.

5 Select the data source type, 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).

6 Upload a sample log file for the data source type you selected in the previous step, then click **Next**.

7 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 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. For information about regular expressions, see Appendix E, Regular Expressions, on page 199. 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)`.

The wizard always contains an extra mapping for the Event Field **name**, which maps all the words in the input log line. ArcSight strongly recommends that you do not simply delete the **name** Event Field but map it in either the Mappings or the Extra Mappings table.

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).

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

Click the **Skip Line** button to go to the next unparsed line in the log file without saving the mapping.

Click the **Skip to End** button to go to the end of the log file without processing any other lines and display the parser file for review.

Click the **Previous** button to go back to the previous line in the log file and make changes if necessary. If you configured any mappings for the previous line, the **Previous** button displays the configured mappings, not the default mappings.

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

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

In Mozilla Firefox, if certain text in the Review Parser File panel is underlined in red, you can disable Spell Check; Right-click in the panel and click **Check Spelling** to remove the check mark.

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

11 Choose how you want to deploy the FlexConnector:

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

  Note: 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 click **Next** to add the parser as a new connector. Follow the steps to add the connector to the container.

Note: After deploying your FlexConnector, you can edit it any time from the **Connectors** tab. See "Editing FlexConnectors" on page 158.

You can share FlexConnectors with other users. See "Sharing Connectors (ArcExchange)" on page 159.

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 6 through Step 11 in "Developing FlexConnectors" on page 155.

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

Tip: In addition to the FlexConnector Edit wizard, you can also use the Edit a File action in the Container Diagnostics wizard to edit your FlexConnector. Refer to "Running Diagnostics on a Container" on page 129.

Sharing Connectors (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 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 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.

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 preconfigured 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 Connector Appliance network settings under Setup > System Admin > Network and that the appliance can communicate with the Protect 724 server.

To package and upload a FlexConnector or parser override:

1. Click **Manage** from the top-level menu bar.
2. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the location in which the connector exists	Click **System** (left panel) > *Location* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the host on which the connector exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Connectors** tab (right panel) > *Name of the Connector* (right panel).
From the Connector page	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > *Container* > *Name of the Connector* (left panel).

3. Click  at the top of the Connector page to open the upload wizard. (From the Connectors page, select the connector in the right panel and click  in the **Action** column.)

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.

Connector Appliance 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 159.

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 will be 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.

To upload the AUP package to ArcExchange, you must have a valid 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.

- 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 153.
- ArcSight recommends that you 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 Connector Appliance network settings under Setup > System Admin > Network and that the appliance can communicate with the Protect 724 server.

To download a FlexConnector or parser override:

1. Click **Manage** from the top-level menu bar.
2. Go to the **Containers** page. Use one of these navigation paths:

User Interface Options	Path
From the System-level page	Click **System** (left panel) > **Containers** tab (right panel).
From the location in which the container exists	Click **System** (left panel) > *Location* (left panel) > **Containers** tab (right panel).
From the host on which the container exists	Click **System** (left panel) > *Location* (left panel) > *Host* (left panel) > **Containers** tab (right panel).

3. In the right panel, select the container into which you want to download the connector, and then click  in the **Action** column to open the download wizard.

4 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.

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.

Preconfigured 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 the Connector Appliance to keep track of the deployment history.

After a successful download, the container is restarted automatically.

To use memory efficiently, parser overrides for the Windows Unified connector only load when the first event is received.

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**: ArcSight recommends that you 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 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 Connector Appliance run as a service (not as an application). Therefore, asset scanner connectors running on Connector Appliance 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.
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. Connector Appliance 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 Connector Appliance users. Refer to "Sharing Connectors (ArcExchange)" on page 159.

For more information, consult the *FlexConnector Developer's Guide*, available from 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 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:

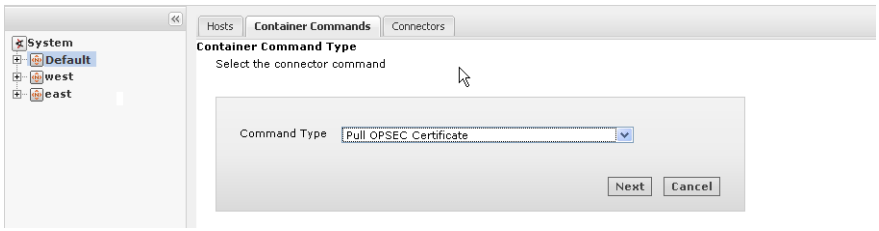
1 Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object.

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.
Host	The hostname of the Connector Appliance .
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 "Running a Command on a Container" on page 125. 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/<container
name>/current/user/agent/checkpoint/<name>. Certificate was
created successfully and written to "/opt/arcsight/<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 the Connector Appliance:

4 Add a Check Point connector by following instructions described in "Adding a Connector" on page 130. 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!
```

Click the **Ignore warnings** check box. Click **Next**.

6 Continue to configure the rest of the connector. Go to Step 6 in "Adding a Connector" on page 130.

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:

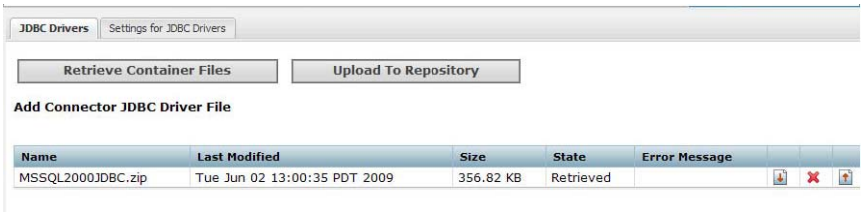
1. Download the MS SQL Server 2005 JDBC Driver 1.2 to a computer that can access Connector Appliance. You can download the driver from Microsoft at:

   `http://www.microsoft.com/downloads/details.aspx?FamilyId=C47053EB-3B64-4794-950D-81E1EC91C1BA&displaylang=en`

2. Run the setup program to install the driver.

3. Follow the instructions in "Uploading Files to a Repository" on page 85 to add the `sqljdbc.jar` file.

   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 87.

   After the driver file has been uploaded to a container, follow the instructions in "Adding a Connector" on page 130 to add a connector that requires a JDBC driver.

Chapter 8

Monitoring the Connector Appliance

The following topics are discussed here.

Monitor Tab Overview

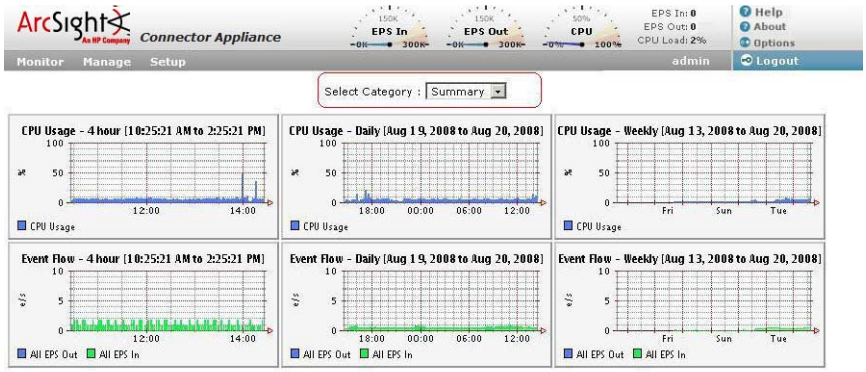
The Monitor tab displays the real-time and historical status of platform- and network-specific aspects of the Connector Appliance, such as CPU, event flow, and disk usage statistics.

Under the Monitor tab, you can select monitor pages for Summary, Platform, or Network. The Platform and Network monitor pages include a duration control. You can choose from these time spans for historical data:

- 4-hours
- Daily
- Weekly

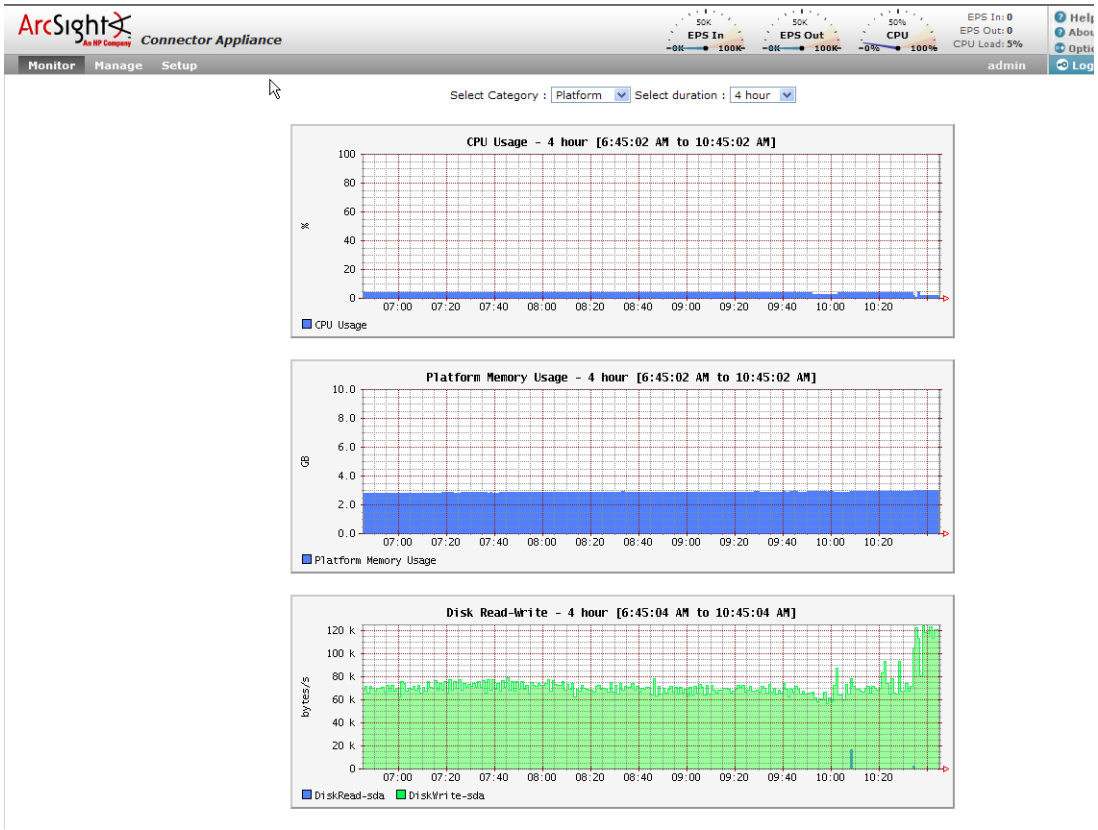
Viewing the Summary Page

The Summary page, shown below, 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.

Appendix A

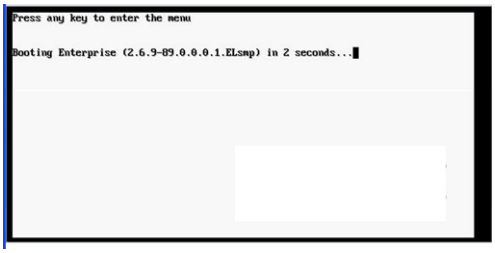
Restoring Factory Settings

You can restore the ArcSight Connector Appliance to its original factory settings using the built-in Acronis True Image software.

Restoring Connector Appliance to factory settings irrevocably deletes all configuration settings.

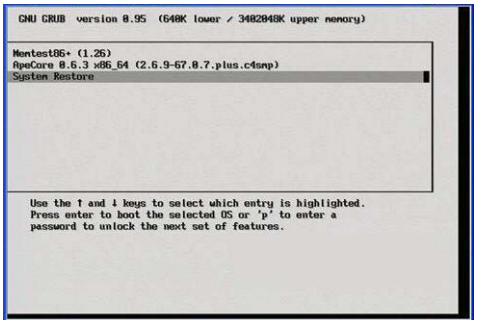
To restore Connector Appliance to the original factory settings:

1. Attach a keyboard, monitor, and mouse directly to the appliance.
2. Reboot Connector Appliance from the GUI. Click **Setup** > **System Admin** > **Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
3. When the following screen displays, press any key on your keyboard.



This screen is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance continues to boot normally.

4. A screen similar to the one shown below appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press Enter.



5 Click **Acronis True Image Server** to continue.

6 In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press Enter.

7 When the Restore Data Wizard starts, click **Next** to continue.

8 On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.

9 On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.

10 On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** or **sda** (depending on the appliance model) and click **Next**.

11 On the **NT Signature selection for image restoration** page, select how you want the NT signature for the restored disk to be processed and click **Next**.

12 On the **Restored Hard disk Location** page, select the drive to restore (**cciss/c0d0** or **sda**) and click **Next**.

13 On the **Non-empty Destination Hard Disk Drive** page, select **Yes, I want to delete all partitions on the destination hard disk drive before restoring** and click **Next**.

14 On the **Next Selection** page, select **No, I do not** and click **Next** (there are no other partitions or disks to restore).

15 On the **Restoration Options** page, select **Validate backup archive for the data restoration process** if you want to validate the archive before resetting the appliance. Select **Reboot the computer automatically after the restoration is finished** if you want to reboot the appliance automatically. Click **Next**.

16 Review the checklist of operations to be performed and click **Proceed** to begin factory reset. Click **Back** to revisit previous pages.

Do not interrupt or power-down Connector Appliance during the reset process. Interrupting the reset process can force the system into a state from which it cannot recover.

Progress bars show the status of the current operation and the total progress.

17 When you see a message indicating that the data was restored successfully, click **OK**.

18 If you specified automatic reboot in Step 15, the appliance reboots when the reset is complete. Otherwise, reboot manually.

Appendix B

Audit Logs

The following topics are discussed here.

Audit Event Types

You can forward the Connector Appliance audit events, which are in Common Event Format (CEF), to a destination of your choice.

Three types of audit events are generated on the Connector Appliance:

- Application events—related to Connector Appliance functions and configuration changes
- Platform events—related to the Connector Appliance hardware/system
- System health events—related to the health of the Connector Appliance

Audit Event Information

A Connector Appliance audit event contains information about the following prefix fields.

- Device Event Class ID
- Device Severity
- Name
- Device Event Category—(key name for this CEF extension is `cat`)

See "Audit Logs" on page 42 for details on how to generate logs.

Configuring Event Forwarding

To configure Connector Appliance to forward application, platform, and 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 audit forwarding on the container.

Follow the procedure below.

To configure event forwarding:

1. Upload an ESM certificate to Connector Appliance so that the appliance and ESM Manager can communicate. To upload the ESM certificate to Connector Appliance, refer to "CA Certs Repository" on page 75.

   For information about SSL Authentication and ESM certificates, see "Understanding SSL Authentication" in the *ArcSight ESM Administrator's Guide*.

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 117.

3 Add the Syslog Daemon connector to the container to which you added the certificate. Refer to “Adding a Connector” on page 130.

When choosing a destination, select **ArcSight Manager (encrypted)**.

If the Syslog Daemon connector already exists in a container, skip Step 1 through Step 3 and go to Step 4.

4 Edit these runtime parameters for the Syslog Daemon connector:

- Set the **Preserve System Health Events** parameter to **Yes**.
- Set the **Enable Device Status Monitoring (in millisec)** parameter to a positive number. The minimum interval is one minute (60,000 milliseconds). Smaller values result in one-minute intervals. If you set this parameter to a negative number, device status monitoring is disabled.

Refer to “Editing Destination Runtime Parameters” on page 147.

5 Configure audit forwarding for the container that has the Syslog Daemon connector. Refer to “Audit Forwarding” on page 43.

Application Events

Signature	Severity	Definition	Category
Connector			
connector:101	1	Connector add successful	/Connector/Add/Success
connector:201	1	Connector add failed	/Connector/Add/Fail
connector:102	1	Connector deleted	/Connector/Delete
connector:202	1	Connector delete failed	/Connector/Delete/Fail
connector:103	1	Connector parameters update successful	/Connector/Parameter/Update/Success
connector:203	1	Connector parameters update failed	/Connector/Parameter/Update/Fail
Destination			
destination:102	1	Destination update to a connector successful	/Connector/Destination/Update/Success
destination:202	1	Destination update to a connector failed	/Connector/Destination/Update/Fail
destination:103	1	Destination delete from a connector successful	/Connector/Destination/Delete/Success
destination:203	1	Destination delete from a connector failed	/Connector/Destination/Delete/Fail
destination:104	1	Destination configuration update successful	/Connector/Destination/Configuration/Update/Success
destination:204	1	Destination configuration update failed	/Connector/Destination/Configuration/Update/Fail
destination:105	1	Register destination successful	/Connector/Destination/Registration/Success
destination:205	1	Register destination failed	/Connector/Destination/Registration/Fail
destination:106	1	Destination configuration add successful	/Connector/Destination/Configuration/Add/Success
destination:206	1	Destination configuration add failed	/Connector/Destination/Configuration/Add/Fail
destination:107	1	Destination configuration delete successful	/Connector/Destination/Configuration/Delete/Success
destination:207	1	Destination configuration delete failed	/Connector/Destination/Configuration/Delete/Fail

Signature	Severity	Definition	Category
Container			
container:101	1	Container upgrade successful	/Container/Upgrade/Success
container:201	1	Container upgrade failed	/Container/Upgrade/Fail
container:301	1	Container upgrade started	/Container/Upgrade/Start
container:102	1	User file push to a container successful	/Container/UserFiles/Push/ Success
container:202	1	User file push to a container failed	/Container/UserFiles/Push/Fail
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
container:204	1	CA cert push to a container failed	/Container/CACert/Push/Fail
container:105	1	Enable demo CA for a container successful	/Container/DemoCA/Enable/ Success
container:205	1	Enable demo CA for a container failed	/Container/DemoCA/Enable/Fail
container:106	1	Disable demo CA for a container successful	/Container/DemoCA/Disable/ Success
container:206	1	Disable demo CA for a container failed	/Container/DemoCA/Disable/ Fail
container:109	1	Delete property from a container successful	/Container/Property/Delete/Success
container:209	1	Delete property from a container failed	/Container/Property/Delete/Fail
container:110	1	Update property to a container	/Container/Property/Update/Success
container:210	1	Update property to a container failed	/Container/Property/Update/Fail
container:111	1	Container password update successful	/Container/Password/Update/ Success
container:211	1	Container password update failed	/Container/Password/Update/ Fail
container:112	1	Container add successful	/Container/Add/Success
container:212	1	Container add failed	/Container/Add/Fail
container:113	1	Container update	/Container/Update
container:114	1	Container delete	/Container/Delete

Signature	Severity	Definition	Category
container:115	1	Add certificate for a container successful	/Container/Certificate/Add/Success
container:215	1	Add certificate for a container failed	/Container/Certificate/Add/Fail
container:116	1	Delete certificate for a container successful	/Container/Certificate/Delete/Success
container:216	1	Delete certificate for a container failed	/Container/Certificate/Delete/Fail
container:117	1	Enable FIPS on a container successful	/Container/FIPS/Enable/Success
container:217	1	Enable FIPS on a container failed	/Container/FIPS/Enable/Fail
container:118	1	Disable FIPS on a container successful	/Container/FIPS/Disable/Success
container:218	1	Disable FIPS on a container failed	/Container/FIPS/Disable/Fail
Location			
location:101	1	Location add successful	/Location/Add/Success
location:201	1	Location add failed	/Location/Add/Fail
location:102	1	Location update	/Location/Update
location:103	1	Location delete	/Location/Delete
Host			
host:101	1	Host add successful	/Host/Add/Success
host:201	1	Host add failed	/Host/Add/Fail
host:103	1	Host delete	/Host/Delete
host:104	1	Host upgrade started	/Host/Upgrade/Start
host:204	1	Host upgrade successful	/Host/Upgrade/Success
host:304	1	Host upgrade failed	/Host/Upgrade/Fail

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:210	3	Global login settings modified	/Platform/Configuration/ Authentication/Login

Signature	Severity	Definition	Category
platform:211	3	Password policy modified	/Platform/Configuration/Authentication/Passwords
platform:212	5	Authentication settings modified	/Platform/Configuration/Authentication/Validation
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:223	5	Certificate request expired	/Platform/Certificate/Expired
platform:225	7	Failed to upload file	/Platform/Update/Failure/Upload
platform:227	5	Applied appliance update	/Platform/Update/Applied
platform:230	5	Successful login	/Platform/Authentication/Login
platform:231	5	Successful login (RADIUS)	/Platform/Authentication/Login/RADIUS
platform:232	7	Failed login attempt (BADUSER)	/Platform/Authentication/Failure/BADUSER
platform:233	7	Failed login attempt (BADPASS)	/Platform/Authentication/Failure/BADPASS
platform:234	7	Failed login attempt (LOCKED)	/Platform/Authentication/Failure/LOCKED
platform:236	7	Failed login attempt (EBADAUTH)	/Platform/Authentication/Failure/EBADAUTH
platform:237	7	Failed login attempt (ETIMEOUT)	/Platform/Authentication/Failure/ETIMEOUT
platform:238	7	Failed login attempt (NOACCESS)	/Platform/Authentication/Failure/NOACCESS
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:243	3	Modified user group membership	/Platform/Groups/Membership/Update
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

Signature	Severity	Definition	Category
platform:249	3	Removed all members from group	/Platform/Groups/Membership/Remove
platform:250	5	Added remote mount point	/Platform/Storage/NFS/Add
platform:251	5	Edited remote mount point	/Platform/Storage/NFS/Edit
platform:252	7	Failed to create remote mount point	/Platform/Storage/NFS/Failure
platform:253	5	Removed remote mount point	/Platform/Storage/NFS/Remove
platform:260	5	Static route modified	/Platform/Configuration/Network/Route/Update
platform:261	5	Static route deleted	/Platform/Configuration/Network/Routes/Remove
platform:262	5	Appliance time modified	/Platform/Configuration/Time
platform:263	5	Network settings modified	/Platform/Configuration/Network
platform:264	5	NTP server settings modified	/Platform/Configuration/Network/NTP
platform:265	5	DNS settings modified	/Platform/Configuration/Network/DNS
platform:266	5	Hosts file modified	/Platform/Configuration/Network/Hosts
platform:268	5	Static route added	/Platform/Configuration/Network/Route/Add
platform:269	5	Updated Platform Settings	/Platform/Configuration
platform:270	9	Stopped process '<process>'	/Platform/Process/Control/Stop
platform:271	7	Restarted process '<process>'	/Platform/Process/Control/Restart
platform:272	5	Started process '<process>'	/Platform/Process/Control/Start
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: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:450	3	FTP service enabled	/Platform/FTP/Enable

Signature	Severity	Definition	Category
platform:451	5	FTP service disabled	/Platform/FTP/Disable
platform:452	3	FTP service started	/Platform/FTP/Start
platform:453	7	FTP service stopped	/Platform/FTP/Stop
platform:454	3	FTP service configuration changed	/Platform/FTP/ConfigurationChange
platform:455	3	Added subdirectory	/Platform/FTP/Subdirectory/Add
platform:456	5	Removed subdirectory	/Platform/FTP/Subdirectory/Remove

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:102	1	Health statistics per disk (read)	/Monitor/Disk/*drive*/Read
disk:103	1	Health statistics per disk (write)	/Monitor/Disk/*drive*/Write
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			
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
network:102	1	Health statistics per network interface (input packets)	/Monitor/Network/Usage/*iface*/PacketsIn
network:103	1	Health statistics per network interface (output packets)	/Monitor/Network/Usage/*iface*/PacketsOut

Signature	Severity	Definition	Category
RAID Controller			
raidcontroller:100	1	Health statistics for the RAID Controller configuration	/Monitor/RAIDController/Configuration/RAID-5
raidcontroller:101	1	Health statistics for RAID Controller port 0	/Monitor/RAIDController/Port/p0
raidcontroller:102	1	Health statistics for RAID Controller port 1	/Monitor/RAIDController/Port/p1
raidcontroller:103	1	Health statistics for RAID Controller port 2	/Monitor/RAIDController/Port/p2
raidcontroller:104	1	Health statistics for RAID Controller port 3	/Monitor/RAIDController/Port/p3
raidcontroller:105	1	Health statistics for the RAID Controller Battery Backup Unit sensor	/Monitor/RAIDController/Sensor/bbu
Sensor			
sensor:100	1	Health statistics for the CPU 1 sensor	/Monitor/Sensor/CPU1
sensor:101	1	Health statistics for the CPU 2 sensor	/Monitor/Sensor/CPU2
sensor:102	1	Health statistics for the system sensor	/Monitor/Sensor/System
sensor:103	1	Health statistics for the DIMM sensor	/Monitor/Sensor/DIMM
sensor:104	1	Health statistics for the CPU1 core sensor	/Monitor/Sensor/CPU1Core
sensor:105	1	Health statistics for the CPU2 core sensor	/Monitor/Sensor/CPU2Core
sensor:106	1	Health statistics for the 3.3V sensor	/Monitor/Sensor/3.3V
sensor:107	1	Health statistics for the 5V sensor	/Monitor/Sensor/5V
sensor:108	1	Health statistics for the 12V sensor	/Monitor/Sensor/12V
sensor:109	1	Health statistics for the -12V sensor	/Monitor/Sensor/-12V
sensor:110	1	Health statistics for the battery sensor	/Monitor/Sensor/Battery
sensor:111	1	Health statistics for the FAN1 sensor	/Monitor/Sensor/FAN1
sensor:112	1	Health statistics for the FAN2 sensor	/Monitor/Sensor/FAN2
sensor:113	1	Health statistics for the FAN3 sensor	/Monitor/Sensor/FAN3

Signature	Severity	Definition	Category
sensor:114	1	Health statistics for the FAN4 sensor	/Monitor/Sensor/FAN4
sensor:115	1	Health statistics for the FAN5 sensor	/Monitor/Sensor/FAN5
sensor:116	1	Health statistics for the FAN6 sensor	/Monitor/Sensor/FAN6
sensor:119	1	Health statistics for the power supply sensor	/Monitor/Sensor/PowerSupply

SNMP Polling of System Health Information

You can poll appliance health information from Connector Appliance using SNMP v2 from any standard network management system. Refer to your appliance's Management Information Base (MIB) at `https://<ConnApp_system_name_or_ip>/platform-service/appliance.mib` for the events you can poll from your system. System health information is exposed using the **applianceSensorTable** object defined in the MIB.

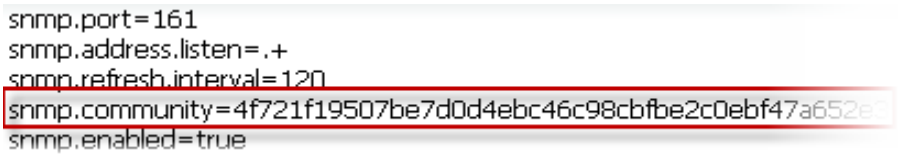
You can only perform the `snmp get`, `getnext`, `getbulk` operations on your system; `snmp set` operations are not permitted.

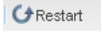
SNMP Configuration

If you wish to alter your SNMP configuration, you can change these elements through the Diagnostic Tools feature.

To set or change your SNMP community string:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Diagnostic Tools** from the **System** section in the left panel to open the Diagnostic Tools page.
3. From the **Tool** drop-down box, choose **Edit text file**.
4. From the **Category** drop-down box, choose **SNMP**.
5. From the **File** drop-down box, choose **SNMP Configuration**.
6. Click the **Edit** button. The SNMP Configuration file appears.

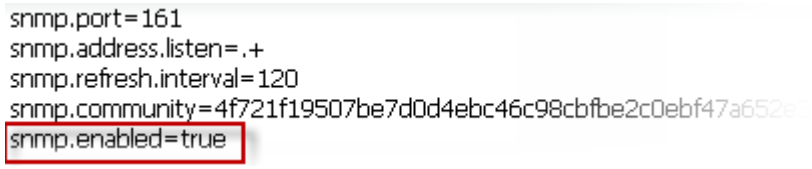


7. Change **snmp.community=** to the desired string.
8. Click the **Save** button.
9. Click **Process Status** from the **System** section in the left panel.
10. Find **snmp** and click the **Restart** button 

to restart SNMP.

To enable/disable SNMP monitoring:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Diagnostic Tools** from the **System** section in the left panel to open the Diagnostic Tools page.
3. From the **Tool** drop-down box, choose **Edit text file**.
4. From the **Category** drop-down box, choose **SNMP**.
5. From the **File** drop-down box, choose **SNMP Configuration**.
6. Click the **Edit** button. The SNMP Configuration file appears.



7. Change **snmp.enabled=** to **true** to enable SNMP or **false** to disable it.
8. Click the **Save** button.
9. Click **Reboot** from the **System** section in the left panel to reboot the system.

Appendix C

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 Destination Parameters" on page 145.

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 ESM 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 ESM 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**.
Don't Resolve Host Names Matching	NA
Don't Reverse-Resolve IP Ranges	NA
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 ESM 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 ESM 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 ESM 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	When populated, this field shows the URI of the zone associated with the connector's source address. This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Source Translated Zone URI	When populated, this field shows the URI of the zone associated with the connector's translated source address. The translation is presumed to be NAT (network address translation). This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Destination Zone URI	When populated, this field shows the URI of the zone associated with the connector's destination address. This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Destination Translated Zone URI	When populated, this field shows the URI of the zone associated with the connector's translated destination address. The translation is presumed to be NAT (network address translation). This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.

Connector Zone URI	When populated, this field shows the URI of the zone associated with the connector's address. This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Connector Translated Zone URI	When populated, this field shows the URI of the zone associated with the connector's translated address. The translation is presumed to be NAT (network address translation). This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Device Zone URI	When populated, this field shows the URI of the zone associated with the device's address. This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
Device Translated Zone URI	When populated, this field shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT (network address translation). This field is present for ESM v3.0 compatibility. It is not relevant in ESM v3.5 because of integral zone mapping.
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 (i.e., 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 (i.e., 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	If your configuration, reporting, and analytic usage permits, you can greatly 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. Consider the possible effects such a restricted data set might have from a given device (e.g., on reports, rules, threat resolution) before selecting it. 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 ESM 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 ESM 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 D
CLI Commands

The following is a complete list of command-line interface (CLI) commands available for Connector Appliance. These commands are useful in configuring the initial platform (system) settings of your Connector Appliance if you connect to it through the serial port or the rear panel connectors.

Command	Description
exit	Log out.
halt	Stop and power down the Connector Appliance.
reboot	Reboot the Connector Appliance.
set date	Sets current date. **Example:** `set date 20101219081533`
set defaultgw <IP> [nic]	Set the default gateway for one or all network interfaces.
set dns <dn1>[,<dn2>, <dn3>] ns1 [ns2]	Set DNS name server(s). dn=search domain name ns=nameserver **Example:** `set dns yourco.com,sales.yourco.com 192.168.10.4`
set hostname <host>	Set the Connector Appliance host name.

set ip <nic> (<IP>/prefix] | <IP> netmask)	Set the Connector Appliance IP address for a specific network interface.
	
	Equivalent examples:
	`set ip eth0 192.168.10.4/24`
	`set ip eth0 192.168.10.4 255.255.255.0`

set password	Set the password for the current user's account.
show admin	Show the default administrator user name.
show config	Show the host name, IP address, DNS, and default gateway for this Connector Appliance.
show date	Shows current date.
show defaultgw [nic]	Display the default gateway for all or the specified network interface.

Command	Description
show dns	Display the DNS name servers currently configured.
show hostname	Display the current hostname.
show ip [nic]	Show the IP addresses of all or the specified network interface.

Appendix E

Regular Expressions

The following topics are covered here.

Overview

A regular expression (regex) is a special text string for describing a search pattern and extracting tokens from a given string. You use java regex in Connector Appliance to develop FlexConnectors with the FlexConnector wizard (see "Developing FlexConnectors" on page 155).

In its simplest form, a regular expression is just a word or phrase to search for. For example, `gauss` matches any event containing the string `gauss` or that mentions the word `gauss`. Events with `gauss`, `gaussian` or `degauss` are all matched in addition to events containing the phrases `de-gauss the monitor` or `gaussian elimination`.

Spaces can be part of the regular expression. For example, `top ten` matches top ten lists. (You also finds articles on how to stop tension.)

Regular expressions can be complex. It can be more work mastering a search than sifting through a long list of matches (even if you are already familiar with regular expressions).

The search is case insensitive; `mopac`, `Mopac`, and `MOPAC` all search for the same set of strings. Each will match `mopac`, `MOPAC`, `Mopac`, `mopaC`, `MoPaC`, `mOpAc` and so on.

Regular Expression Constructs

Table E-1 Meta-characters

Meta-Character	Definition	Pattern	Sample Matches
`.`	Any character (except `\n` - new-line).	`a.c`	`abc, aac, acc, adc, aec, ...`
`|`	Alternation.	`bill|ted`	`ted, bill`
`{...}`	Explicit quantifier notation.	`ab{2}c`	`abbc`
`[...]`	Explicit set of characters to match.	`a[bB]c`	`abc, aBc`
`(...)`	Logical grouping of part of an expression. The contents of the parentheses are extracted.	`(abc){2}`	`abcabc`
`*`	0 or more of previous expression.	`ab*c`	`ac, abc, abbc, abbbc, ...`
`+`	1 or more of previous expression.	`ab+c`	`abc, abbc, abbbc, ...`
`?`	0 or 1 of previous expression; also forces minimal matching when an expression might match several strings within a search string.	`ab?c`	`ac, abc`
`\\`	Preceding one of the above, making it a literal instead of a special character. Preceding a special matching character, see below.	`a\\sc`	`a c`

Table E-2 Escape Characters

Escape Character	Description
ordinary characters	Characters other than `. $ ^ { [ ( | ) ] } * + ? \` match themselves.
`\t`	Matches a tab `\u0009`.
`\r`	Matches a carriage return `\u000D`.
`\n`	Matches a new line `\u000A`.
`\\x20`	Matches an ASCII character using hexadecimal representation (exactly two digits).
`\\*`	When followed by a character that is not recognized as an escaped character, matches that character.

Table E-3 Character Classes

Character Class	Description
`[aeiou]`	Matches any single character included in the specified set of characters.
`[^aeiou]`	Matches any single character not in the specified set of characters.
`[0-9a-fA-F]`	Use of a hyphen (`–`) allows specification of contiguous character ranges.
`\\w`	Matches any word character.
`\\W`	Matches any non-word character.
`\\s`	Matches any white-space character.
`\\S`	Matches any non-white-space character.
`\\d`	Matches any decimal digit. Equivalent to `[0-9]`.
`\\D`	Matches any non-digit. Equivalent to `[^0-9]`.

Combining Meta-characters

You can combine several metacharacters in one regular expression. The table below provides examples.

Table E-4 Combining Metacharacters

Regular Expression	Description
a\\.*z	Matches any string starting with a, followed by a series of periods (including the series of length zero), and terminated by z. For example, az, a.z, a..z, a...z and so on, are all matched.
a.*z	Matches any string starting with an a, followed by one arbitrary character, and terminated with *z. Therefore, ag*z, a5*z and a@*z are all matched. Only strings of length four, where the first character is a, the third *, and the fourth z, are matched.
a\\++z	Matches any string starting with a, followed by a series of plus signs, and terminated by z. You need at least one plus sign between the a and the z. Therefore, az is not matched, but a+z, a++z, a+++z, and so on are matched.
a\\+\\+z	Matches only the string a++z.
a+\\+z	Matches any string starting with a series of a, followed by a single plus sign and ending with z. You need at least one a at the start of the string. Therefore, a+z, aa+z, aaa+z, and so on match, but +z does not.
a.?e	Matches ace, ale, axe, and any other three-character string beginning with a and ending with e (it also matches ae).
a\\.?e	Matches ae and a.e. No other string is matched.
a.\\?e	Matches any four-character string starting with a and ending with ?e. Therefore, ad?e, a1?e, and a%?e are matched.
a\\.\\?e	Matches only a.?e.

Appendix F

Troubleshooting Tips and FAQs

The following topics are discussed here.

Troubleshooting Tips

This section provides tips that help you troubleshoot issues you might encounter when using Connector Appliance.

Manage Page Takes Too Long to Load

On a Connector Appliance managing a large number of remote containers, a downed connector results in a considerable lag in loading the page. This occurs because the appliance must wait until it receives a “connection refused” error, which can take up to 5 minutes. This wait is repeated for each downed container, resulting in the lag.

Resolution

The page will eventually load. You can also click on the individual locations or hosts from the System tree to load the containers and view the downed connectors. The hosts with successfully running containers will load immediately.

Unable to Add a Secondary Destination

If you get a Java exception when adding a secondary destination, this occurs because a .csv file from a WUC connector has been imported from one container into another. In such cases, the .csv has passwords that are obfuscated by its original container. Each container has differing JVMs, so they cannot unobfuscate a password that was obfuscated by a different container.

Resolution

Open the .csv file in a spreadsheet program and, in plain text, retype the correct passwords for all the hosts. When the .csv is imported into another container, the new container can obfuscate/unobfuscate using its own algorithm.

Unable to Load MS SQL Server Driver

`Unable to load com.microsoft.jdbc.sqlserver.sqlserver`

If you see the above error message when configuring a connector that uses the MS SQL Server Driver for JDBC (such as, McAfee ePO DB, Microsoft SQL Audit, or IBM SiteProtector DB), the incorrect MS SQL JDBC driver is installed on the Connector Appliance.

Resolution

Follow these steps:

- Download the correct version of the MS SQL Server JDBC driver from Microsoft to a computer from which you can access Connector Appliance and unzip the file. Refer to the Configuration Guide for the connector for detailed information.
- Upload the required `sqljdbc.jar` files from the downloaded zip file to the JDBC Drivers repository on the Connector Appliance (**Setup** > **Repositories** > **JDBC Drivers**).
- From the JDBC Drivers repository, upload the driver to the container where you want to install the connector.

These procedures are described in “Adding the MS SQL Server JDBC Driver” on page 168.

Unable to Authenticate to Remote Software Connectors

Connector Appliance can manage connectors running on any network-accessible host. To connect to a software connector for the first time, Connector Appliance uses the default username `connector_user` and the default password `change_me`. After the Connector

Appliance authenticates, you can change the default password (see "Changing Container Credentials" on page 115).

When you change the password, Connector Appliance creates a hash value for the new password in the `agent.properties` file on the software connector. If you delete the hashed password from the `agent.properties` file, Connector Appliance tries to authenticate using the default password and is unsuccessful.

Resolution

To authenticate to the software connector:

1. Open the following file for the connector on the computer where the connector is installed and remove the new password.
   `/opt/arcsight/connector_x/current/user/agent/agent.properties`
2. Add the connector to Connector Appliance again.

   Connector Appliance authenticates successfully with the default password.
3. Change the default password again (see "Changing Container Credentials" on page 115).

HTTP Status 404 Error

```
HTTP Status 404 - /conapp/WEB-INF/jsp/connector_type_config.jsp
type Status report message /conapp/WEB-INF/jsp/
connector_type_config.jsp description The requested resource
(/conapp/WEB-INF/jsp/connector_type_config.jsp) is not available.
```

If you see the above error message when adding a host for a software connector you want to manage remotely, Connector Appliance is unable to resolve the hostname of the computer where the connector is running.

Resolution

In the Connector Appliance hosts file (**Setup** > **System Admin** > **Network** > **Hosts**), add an entry for the computer where the connector is running. See "Hosts" on page 28.

Process Status Displays Execution Failed, but Connectors Are Running

If the process status (**Setup** > **System Admin** > **System** > **Process Status**) shows **Execution Failed**, **Does Not Exist**, or **Not Monitoring**, but the connector status shows **Initialized** or **Connected**, the process status and the connector status are not synchronized. Even though the processes are out of synch, the connector is running and processing events.

The process status is specific to the watchdog monitor process known as monit, not the connector or container status. However, monit does monitor the status of the container processes and sends a command to restart a container process if it becomes unresponsive.

Resolution

To synchronize the process status and the connector status, you need to obtain command-line access to the appliance, then send commands to restart the container and reset the watchdog monitor status:

1. To obtain command-line access to Connector Appliance, refer to "SSH Access to the Appliance" on page 33.
2. From the command line, enter the following commands to restart the container and reset the watchdog monitor status:

   ```
   /opt/local/monit/bin/monit stop connector_x
   ```

   ```
   /etc/init.d/arc_appliance_connector_x start
   ```

   ```
   /opt/local/monit/bin/monit start connector_x
   ```

   where *x* is the number of the container you want to restart.
3. Check the startup progress using the following command:

   ```
   /opt/local/monit/bin/monit summary
   ```
4. After a few moments, the status changes to **Initialized**, then **Running**. The watchdog monitor and the connector status are now synchronized.

Login Failed for sqluser

```
Login failed for user sqluser. The user is not associated with a
trusted SQL server connection.
```

If you see the above error message when you configure the Microsoft 2005 JDBC 1.2 Driver on Connector Appliance for a connection to a Microsoft SQL Server, the Microsoft SQL Server is configured incorrectly for authentication.

The JDBC driver does not support integrated authentication on non-Windows operating systems or any functionality to supply Windows authentication credentials, such as user name and password. Connector Appliance uses a Linux-based operating system.

Resolution

Configure the Microsoft SQL Server for **Mixed Mode Authentication** or **SQL Server Authentication**.

Local Connectors Are Caching Events but Not Remote Connectors

Connectors installed on the local Connector Appliance are caching events, but other connectors installed on a remote Connector Appliance and sending to the same destination are not caching events.

This problem occurs when the Connector Appliance is configured with a DNS server for resolution and the DNS server becomes unavailable. You might see the following symptoms:

- Event flow stops from the local connector to the destination.
- When viewing the connector statistics on the Connector tab, the cached events for that destination are increasing.
- The `/opt/arcsight/connector_x/current/logs/agent.log` file from the container where the connector is installed contains messages similar to the following:

```
[2011-02-01
08:40:11,757][ERROR][default.com.arcsight.agent.transport.a.f][
setIsUp] com.arcsight.agent.transport.e: Ping failed -- last
successful at 1270471156741
[2011-02-01
08:40:11,758][ERROR][default.com.arcsight.agent.loadable.transp
ort.event._AgentLoggerSecureEventTransport][transportSecurityEv
ents] Non-OK IPM response: [java.net.UnknownHostException
during HTTP communication: arcsight.host1.com.] (-1) when
sending 100 events [2011-02-01
08:40:11,758][ERROR][default.com.arcsight.agent.transport.d.t][
run] com.arcsight.agent.transport.e: Non-OK IPM response:
[java.net.UnknownHostException during HTTP communication:
arcsight.hosts1.com.] (-1) when sending 100 events
```

Resolution

Add the IP address and hostname of each destination host to the host table on the Connector Appliance. Refer to “Hosts” on page 28.

Error Messages When Upgrading a Container

```
Upgrade results [//Default/Localhost/Container 1] to version
[x.x.x] Skipped (Container may not be running)
```

If you see the above error message when upgrading a container but the connector in the container is running and processing events, the container is not **Initialized** and Connector Appliance cannot perform the upgrade. Restarting the container does not resolve the problem.

Resolution

Follow the steps below.

To resolve the upgrade problem:

1. Click on the connector under the container from the navigation tree and view the connector details.
2. After viewing the connector details, the container state changes to **Initialized**.
3. Upgrade the container again.

   The container upgrades successfully.

The Containers Tab Takes a Long Time to Load

If you click the **Containers** tab for a remote Connector Appliance or a software host and the page takes a long time to load or you see that the status shows in process for a long time, the remote host might not be reachable.

Resolution

Wait until the remote host becomes available for the Containers tab to load.

Connector Communication Issues

If your connectors are unable to communicate with an ArcSight Manager and you are:

- Using a demo certificate on ArcSight Manager

  Enable the demo certificate on the container where the connectors are located. See "Enabling or Disabling a Demo Certificate on a Container" on page 121 for detailed instructions.

- Using a "self signed" certificate on ArcSight Manager

  Add a CA certificate on the container where the connectors are located. See "Managing Certificates on a Container" on page 117 for detailed instructions.

  After you enable or disable FIPS mode on a container, check that the appropriate certificates are present in the trust store so that the connectors can validate their configured destinations successfully.

If you see an error message indicating that the ESM Manager certificate is not trusted, connectors in FIPS mode are trying to communicate with an ESM Manager that is in non-FIPS mode. Disable FIPS mode on the container. See "Enabling and Disabling FIPS on a Container" on page 116.

- Unable to resolve a hostname

  Update the Hosts file to include the required hostname. See "Hosts" on page 28 for detailed instructions.

Frequently Asked Questions (FAQs)

This section provides answers to frequently-asked questions.

How do you configure connectors to use the Microsoft SQL Server Driver for JDBC?

See "Adding the MS SQL Server JDBC Driver" on page 168.

How do you apply a parser override?

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 apply a parser override, refer to "Adding Parser Overrides" on page 95.

How do you prevent a container with no connectors from starting?

You cannot prevent a container from starting; However, if a container is empty, you can save resources by reducing the memory used for the container to prevent it from starting.

To reduce the memory used for a container:

1. Click **Manage** from the top-level menu bar.
2. Click **System** (left panel) > **Containers** tab (right panel).
3. Click  in the Action column of the container to open the Send Command wizard.
4. Click **Next** to start the wizard.
5. Select the command **Configure Memory Settings** and click **Next**.
6. From the **Heap Memory** field, select **64mb** and click **Next**.
7. Click **Done** to exit the wizard and restart the container.

Make sure you increase the memory when you add connectors to the container.

How do you retrieve connector logs?

You can retrieve logs from connectors and view them on Connector Appliance. Refer to "Viewing Container Logs" on page 127.

How do you manage software connectors on remote hosts?

In addition to the connectors installed on the local appliance, Connector Appliance can manage connectors that are installed on a different computer on your network (remote software connectors). To manage remote software connectors, you need to add the hosts on which those connectors are running to connector Appliance.

To manage a remote connector:

1. Install the connector on the remote host. Follow the instructions in the Configuration Guide for the connector.
2. After completing the installation, open the file `/opt/arcsight/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 the Connector Appliance.

   Note

   - 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. ArcSight recommends a port in the range 9001 - 9020.
   - If you want to manage more than one software connector, you must specify sequential ports; for example, 9002, 9003, 9004.

3. Restart the connector service.
4. From the Connector Appliance GUI, click **Manage** from the top-level menu bar.
5. In the left panel, click the location where you want to install the host.

   On the **Hosts** tab in the right panel, click  at the top of the page to open the Add Host wizard.
6. Provide the remote host parameters in the fields provided:
   a. In the **Hostname / IP** field, enter the hostname or IP address of the computer on which the remote connector is installed.
   b. In the **Starting Port** field, enter the port number you provided in Step 2.
   c. In the **User** field, enter the default username **connector_user** and in the **Password** field, enter the default password **change_me**.
   d. In the **Hardware Type** drop-down box, select **Software**.
7. Click **Next** and then click **Done** to exit the wizard.

   The host and connector name appear in the host tree on the left side. Connector Appliance creates the container automatically.
8. Change the default username and password you specified in Step c. Refer to "Changing Container Credentials" on page 115.

How do you configure multiple syslog connectors?

By default, you can install only one Syslog connector on Connector Appliance; port 514 can be used by only one connector. If you need to install multiple Syslog connectors on a single appliance, you can do so in the following ways:

- Configure additional syslog connectors to use a network port other than the default.
- Install a second syslog connector using the IP address of the second network interface card on the appliance. After you configure the second NIC card (eth1), you can configure a second syslog connector on the same appliance on the default port 514.

To use a network port other than the default:

1. Change the **Network Port** parameter for each additional syslog connector:
   a. In the Connector Appliance GUI, click **Manage** from the top-level menu bar.
   b. In the left panel, click **System** > **Default** > **Localhost** > **Container** > ***Syslog_connector_name***.
   c. On the **Connector** tab in the right panel, click ( ) in the **Connector Parameters** section to open the Edit Connector Parameters wizard.
   d. In the **Network Port** field, enter the network port you want to use for the connector and click **Next**.

      The syslog connector listens for syslog events on the specified network port.
   e. Click **Done** to close the Edit Connector Parameters wizard.
2. Make sure that all devices sending syslog events to this connector are configured to forward events to the port you configured.
3. Make sure that the port you configured is open on the firewall.

To use the IP address of the second network interface card on the appliance:

1. Configure the second network interface on the appliance:
   a. Click **Setup** > **System Admin** from the top-level menu bar.
   b. Click **Network** from the **System** section in the left panel.
   c. On the **Network** tab, enter the IP address for interface eth1, then click **Update Settings**.
   d. Make sure the physical NIC on the appliance is enabled and the appropriate cable is connected.
2. Set the IP address for the additional syslog connector:
   a. Click **Manage** from the top-level menu bar. In the left panel, click **System** > **Location** > **Host** > **Container** > ***Syslog_connector_name***.
   b. On the **Connector** tab in the right panel, click ( ) in the **Connector Parameters** section to open the Edit Connector Parameters wizard.
   c. In the **IP Address** field, enter the IP address that you configured for eth1 in Step c instead of using the default option **ALL**.

      The syslog connector listens for syslog events only on the specified IP address.

Glossary

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C

CAC
Common Access Card. The standard identification card for active duty members of the Uniformed Services, Selected Reserve, DOD civilian employees, and eligible contractor personnel.

Container
A single Java Virtual Machine (JVM) that can run up to four SmartConnectors. A default number of containers exist on each Connector Appliance. The number depends on the Connector Appliance hardware platform. Each container is identified with a label (Container Name) and an associated port number (9001 or higher).

Connector
See SmartConnector.

E

ESM
ArcSight™ Enterprise Security Management. A comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

Event
A record of activity that takes place on a network, OS, application, physical security system, or database.

F

FIPS 140-2
Federal Information Processing Standard 140-2. A standard published by the National Institute of Standards and Technology (NIST), used to accredit cryptographic modules in software components.

FlexConnector
A custom connector that you define to gather security events from log files, databases, and other software and device.

H

Host
A computer on a network that is associated with an IP address, on which connectors are installed. A host can be one of three types: the Localhost, a remotely-managed Connector Appliance, or a software-type host.

L

Location
A logical grouping of hosts. The grouping can be based on any suitable abstraction—geographical, organizational, and so on. For example, you can group all hosts in New York separately from hosts in San Francisco and label them as such. Similarly, you can group a few machines under Sales and others under Marketing.

A location can contain any number of hosts. **Default Location** exists by default on a brand new Connector Appliance; it is empty and cannot be deleted.

Logfu
A diagnostic tool that parses ArcSight logs to generate an interactive visual representation of the information contained within the logs.

Logger
A hardware log management solution that is optimized for extremely high event throughput. An event is a time-stamped text message, either a syslog message sent by a host or a line appended to a log file. Logger receives and stores events; supports search, retrieval, and reporting; and can optionally forward selected events.

P

Parser override
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.

Protect 724
The ArcSight online community. You can access Protect 724 from Connector Appliance to upload and download FlexConnectors and parser overrides.

S

SmartConnector
An ArcSight software component that collects events and logs from various sources on your network. A SmartConnector (also called a connector) can be configured on the Connector Appliance or can be installed on a computer on your network and managed remotely through the Connector Appliance.

SSL
Secure Sockets Layer. The Connector Appliance uses SSL technology to communicate with users using the https protocol.

System
The root view of the Connector Appliance. It enables you to view the hierarchical organization of all the locations, hosts, containers, and connectors on an appliance. **System** exists by default on a brand new Connector Appliance. It cannot be deleted.

Index