

# ArcSight ESM Administrator's Guide

---

ArcSight™ ESM Version 5.0 SP2

September 2011



## ArcSight ESM Administrator's Guide ArcSight™ ESM Version 5.0 SP2

Copyright © 2011 ArcSight, LLC All rights reserved.

ArcSight and the ArcSight logo are registered trademarks of ArcSight in the United States and in some other countries. Where not registered, these marks and ArcSight Console, ArcSight ESM, ArcSight Express, ArcSight Manager, ArcSight Web, ArcSight Enterprise View, FlexConnector, ArcSight FraudView, ArcSight Identity View, ArcSight Interactive Discovery, ArcSight Logger, ArcSight NCM, SmartConnector, ArcSight Threat Detector, ArcSight TRM, and ArcSight Viewer, are trademarks of ArcSight, LLC. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

### Revision History

Date	Product Version	Description
08/24/11	ArcSight ESM Version 5.0 SP2	Bug fixes

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	<a href="mailto:support@arcsight.com">support@arcsight.com</a>
Support Web Site	<a href="http://www.arcsight.com/supportportal/">http://www.arcsight.com/supportportal/</a>
Protect 724 Community	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

# Contents

---

<b>Chapter 1: Basic Administration Tasks .....</b>	<b>9</b>
Running ArcSight ESM .....	9
Starting the ArcSight Manager .....	9
ArcSight Manager Decoupled Process Execution .....	10
Starting the ArcSight Console .....	10
Setting up a Custom Login Message .....	11
Starting ArcSight SmartConnectors .....	11
Stopping the ArcSight Manager .....	12
Reconnecting to the ArcSight Manager .....	12
Configuring ArcSight Manager or ArcSight Web as a Service .....	12
ArcSight Manager Service Setup on Windows .....	12
Starting and Stopping the ArcSight Manager Service on Windows .....	12
Removing the ArcSight Manager Service on Windows .....	13
ArcSight Manager or ArcSight Web Service Setup on Unix Platforms .....	13
Reducing Impact of Anti-Virus Scanning .....	14
License Tracking and Auditing .....	14
Licensed EPS Compliance .....	14
<b>Chapter 2: Configuration .....</b>	<b>17</b>
Managing and Changing Properties File Settings .....	17
Property File Format .....	17
Defaults and User Properties .....	17
Editing Properties .....	18
Dynamic Properties .....	19
Example .....	20
Changing Manager Properties Dynamically .....	21
Changing the Service Layer Container Port .....	22
Securing the ArcSight Manager Properties File .....	22
Adjusting Console Memory .....	22
Adjusting Pattern Discovery Memory .....	23
Installing New License Files Obtained from ArcSight .....	23
Installing in Silent Mode .....	24
Configuring ArcSight Manager Logging .....	24
Sending logs and diagnostic information to ArcSight .....	25

---

Guidelines for using the Send Logs utility .....	25
Gathering logs and diagnostic information .....	26
Understanding SSL Authentication .....	34
Terminology .....	35
Tools for SSL configuration .....	39
Keytoolgui .....	39
keytool .....	43
tempca .....	44
How SSL Works .....	44
SSL certificates .....	46
Types .....	46
Comparing Self-signed and CA-signed certificates .....	46
Using a Demo Certificate .....	47
Using a Self-Signed Certificate .....	48
When clients communicate with one ArcSight Manager .....	48
When clients communicate with multiple ArcSight Managers .....	50
Using a CA-Signed Certificate .....	52
Obtaining a CA-signed certificate .....	52
Importing a CA-signed certificate into Manager's truststore .....	54
Replacing an Expired Certificate .....	56
Establishing SSL Client Authentication .....	57
Setting up SSL Client-Side Authentication on ArcSight Console running in Default Mode .	57
Setting up SSL Client Authentication on ArcSight Web .....	65
Setting up Client-side Authentication on Partition Archiver and SmartConnectors .....	69
Migrating from one certificate type to another .....	72
Migrating from Demo to Self-Signed .....	72
Migrating from Demo to CA-Signed .....	72
Migrating from Self-Signed to CA-Signed .....	73
Verifying SSL Certificate Use .....	73
Sample output for verifying SSL certificate use .....	73
Using Certificates to Authenticate Users to ArcSight .....	74
Using the Certificate Revocation List (CRL) .....	74
Reconfiguring the ArcSight Console after Installation .....	75
Reconfiguring ArcSight Manager .....	75
Changing ArcSight Manager Ports .....	76
Changing ArcSight Web Session Timeouts .....	76
Manager Password Configuration .....	76
Enforcing Good Password Selection .....	76
Password Length .....	76
Restricting Passwords Containing User Name .....	77
Requiring Mix of Characters in Passwords .....	77
Checking Passwords with Regular Expressions .....	78
Password Uniqueness .....	78

---

Setting Password Expiration .....	79
Restricting the Number of Failed Log Ins .....	79
Re-Enabling User Accounts .....	80
Properties Related to Domain Field Sets .....	80
Advanced Configuration Options for Asset Auto-Creation .....	81
Asset Auto-Creation from Scanners in Dynamic Zones .....	81
Create Asset if either IP Address or Host Name .....	81
Preserve Previous Assets .....	82
Changing the Default Naming Scheme .....	83
Compression and Turbo Modes .....	84
Enabling Compression for ArcSight SmartConnector Events .....	84
Understanding ArcSight Turbo Modes .....	84
Configuring the ArcSight Database Monitor .....	85
Configuring Database Monitor e-mail message recipients .....	86
Configuring the check for free space in Oracle tablespaces .....	86
Sending Events as SNMP Traps .....	86
Configuration of the SNMP trap sender .....	86
Asset Aging .....	88
Excluding Assets From Aging .....	88
Task to Disable Assets of a Certain Age .....	88
To Delete an Asset .....	89
Amortize Model confidence with scanned asset age .....	89
<b>Chapter 3: Database Administration .....</b>	<b>91</b>
Changing Oracle Initialization Parameters .....	91
Monitoring Available Free Space in Tablespaces .....	92
Setting Up Database Threshold Notification .....	92
Resetting the Oracle Password .....	92
Backing up ArcSight Databases .....	93
Oracle Cold Backup .....	93
Oracle Hot Backup .....	93
Exporting Data .....	94
Recovering ArcSight Databases .....	94
Speeding up partition compression .....	94
Partition logs .....	95
<b>Chapter 4: Managing Resources .....</b>	<b>97</b>
<b>Appendix A: ArcSight Commands .....</b>	<b>99</b>
Running an ArcSight Command Script .....	99
Alphabetic List of Commands .....	100
<b>Appendix B: Troubleshooting .....</b>	<b>155</b>
General .....	155

---

Query and Trend Performance Tuning .....	158
Regenerate Event Statistics .....	158
Persistent Database Hints .....	159
server.defaults.properties Entries for Trends .....	159
Troubleshooting Checklist after Restarting the Manager .....	159
Reports for Monitoring Trend Performance .....	159
Disable these Trends on High Throughput Systems .....	160
How will you know when a trend is caught up? .....	160
How long will it take a trend to catch up? .....	160
Enhancing the Performance Globally for all Database Queries .....	161
SmartConnectors .....	161
Console .....	162
Manager .....	164
ArcSight Web .....	165
Database .....	166
SSL .....	167
Cannot connect to the SSL server: IO Exception in the server logs when connecting to the serv- er .....	167
Cannot connect to the SSL server .....	167
PKIX exchange failed/could not establish trust chain .....	167
Issuer certificate expired .....	167
Cannot connect to the Manager: Exception in the server log .....	168
Certificate is invalid .....	168
Issue with Internet Explorer and ArcSight Web in FIPS Mode .....	168
<b>Appendix C: Monitoring Database Attributes .....</b>	<b>169</b>
Understanding Database Checks .....	169
Message text .....	169
Disabling Database Checks .....	171
List of Database Check Tasks .....	171
<b>Appendix D: The Logfu Utility .....</b>	<b>175</b>
Running Logfu .....	176
Example .....	178
Troubleshooting .....	178
Menu .....	180
Typical Data Attributes .....	180
Intervals .....	181
<b>Appendix E: Creating Custom E-mails Using Velocity Templates .....</b>	<b>183</b>
Overview .....	183
Notification Velocity templates .....	183
Commonly used elements in Email.vm and Informative.vm files .....	183
The #if statement .....	183

---

Contents of Email.vm and Informative.vm .....	184
How the Email.vm and Informative.vm Template Files Work .....	185
Understanding the Customization Process .....	185
Customizing the template files .....	186
Sample Output .....	187
<b>Appendix F: The Archive Command Tool .....</b>	<b>189</b>
Overview of the Archive Command Tool .....	189
Exporting Resources to an Archive .....	190
Importing Resources from an Archive .....	191
About Importing v3.x Content to a v4.x ESM System .....	192
Syntax for Performing Common Archive Tasks .....	194
<b>Appendix G: TLS Configuration to Support FIPS Mode .....</b>	<b>197</b>
NSS Tools Used to Configure Components in FIPS Mode .....	198
Types of Certificates Used in FIPS Mode .....	198
Using a Self-Signed Certificate .....	199
Using a Certificate Authority (CA) Signed Certificate .....	199
Steps Performed on the Manager .....	199
Steps Performed on the Web .....	203
Steps Performed on the Console .....	208
Some Often Used SSL-related Procedures .....	212
Generating a Key Pair in a Component's NSS DB .....	212
On the Manager .....	212
On the Console .....	213
On ArcSight Web .....	214
Verifying Whether the Key pair Has Been Successfully Created .....	214
Viewing the Contents of the Certificate .....	214
Exporting a Certificate .....	215
From the Manager .....	215
From the Console .....	215
From the Web .....	215
Importing a Certificate into NSS DB .....	216
On the Manager .....	216
On the Console .....	217
On ArcSight Web .....	217
Importing an Existing Key Pair into the NSS DB .....	217
Setting up Server-Side Authentication .....	218
Setting up Client-Side Authentication .....	218
Changing the Password for NSS DB .....	220
Listing the Contents of the NSS DB .....	221
Viewing the Contents of a Certificate .....	221
Setting the Expiration Date of a Certificate .....	221

---

Deleting an Existing Certificate from NSS DB .....	222
Replacing an Expired Certificate .....	222
Using the Certificate Revocation List (CRL) .....	223
Migrating an Existing Default Mode ESM Installation to FIPS Mode .....	223
<b>Appendix H: Monitoring System Health .....</b>	<b>225</b>
Overview .....	225
What to Monitor .....	225
ArcSight Appliances .....	226
ArcSight ESM .....	227
ESM Component Configuration .....	228
Configuring SmartConnectors .....	228
Configuring the Connector Appliance .....	228
Configuring Logger .....	229
Configuring ESM .....	229
ESM Content Configuration .....	229
Configure Critical Device Not Reporting Resources .....	229
Configure White List Filters .....	230
Configure Critical Device Not Reporting Rule .....	232
Configure Connector Monitoring Resources .....	232
Configuring Active Lists for Connector Information and Up or Down Status .....	234
Rules Relating for Connector Up or Down Status .....	234
<b>Index .....</b>	<b>237</b>



# Chapter 1

## Basic Administration Tasks

---

This chapter describes the various tasks that you can perform to effectively manage an ArcSight ESM installation, performing additional configuration and maintenance operations for ArcSight Manager and the database.

The following topics are covered here:

- ["Running ArcSight ESM" on page 9](#)
- ["Starting the ArcSight Manager" on page 9](#)
- ["Starting the ArcSight Console" on page 10](#)
- ["Starting ArcSight SmartConnectors" on page 11](#)
- ["Stopping the ArcSight Manager" on page 12](#)
- ["Reconnecting to the ArcSight Manager" on page 12](#)
- ["Configuring ArcSight Manager or ArcSight Web as a Service" on page 12](#)
- ["Reducing Impact of Anti-Virus Scanning" on page 14](#)
- ["License Tracking and Auditing" on page 14](#)

## Running ArcSight ESM

Unless ArcSight ESM is configured to run as a service, you run ArcSight Manager, Console, and SmartConnectors using the Start menu. For Linux and Solaris, you need to start the ArcSight Manager from a command or console window, or set up ArcSight Manager as a daemon. The remainder of this section provides more information about command line options you can use to start up, shut down, configure, or reconfigure ESM components. In addition, it provides information about setting up ArcSight Manager as a daemon (on Unix platforms) or as a service (on Windows), if you didn't originally configure ArcSight Manager that way.

## Starting the ArcSight Manager

To start ArcSight Manager from the command line, if it's not configured to run either as a daemon or a service:

- 1 Open a command window or terminal box.
- 2 Change directories to the ArcSight Manager `bin` directory:
- 3 Type in the following line and press **Enter**.

```
./arcsight manager
```

When it starts, the ArcSight Manager will display a stream of messages in the command window or terminal box to reflect its status. The command window or terminal box will say Ready when the Manager has started successfully. If you are starting the Manager as a service, you can monitor whether or not it has successfully loaded by viewing the `server.std.log` file, located in `<ARCSIGHT_HOME>\logs\default` on Windows. On Unix systems, you can use the command:

`cd ARCSIGHT_HOME;tail -f logs/default/server.std.log`On Windows systems, you can use a “tail” equivalent tool to run the same command, such as those available from <http://www.cygwin.com>, which provides Unix environments and tools for Windows.



Closing the command prompt or terminal box in which ArcSight Manager was started, or pressing CTRL-C keys in the window, will initiate a controlled and graceful shut down of the ArcSight Manager.

---

## ArcSight Manager Decoupled Process Execution

On UNIX-based systems, ArcSight Manager uses decoupled process execution to perform specific tasks, for example to compile rulesets, either on initial startup or when the real-time rules group changes. To do so, ArcSight Manager uses a standalone process executor (instead of using “in process” or “direct process” execution). ArcSight Manager sends commands to be executed via the file system. The process executor uses the `<ARCSIGHT_HOME>/tmp` directory, so you should restrict system level access for this directory.

The process executor is used, by default, on all Unix platforms. The ArcSight Manager scripts ensure that the Process Executor will be executed as a daemon before the ArcSight Manager is started. This has some implications with regards to troubleshooting ArcSight Manager startup and runtime problems. The ArcSight Manager, if configured to use the Process Executor, will not start if the presence of a running Process Executor cannot be detected. The Process Executor runs within its own watchdog, in the same fashion as the ArcSight Manager, so if the process stops for any reason, it will restart automatically. The process executor is transparent to users regarding the way that ArcSight Manager is started or stopped.

The `stdout` and `stderr` of the executed process will be written into the following two files:

`<ARCSIGHT_HOME>/tmp/[commandfile-name].stdout`

`<ARCSIGHT_HOME>/tmp/[commandfile-name].stderr`

## Starting the ArcSight Console

Before you start ArcSight Console or SmartConnectors, be sure ArcSight Manager is installed and has completed a successful startup. To start up the ArcSight Console:

- 1 Open a command window or shell window on `<ARCSIGHT_HOME>/bin`.
- 2 Type in the following line and press **Enter**.  
`./arcsight console`

## Setting up a Custom Login Message

You can configure the ArcSight Manager to display a custom message before allowing users to log in to the Console or ArcSight Web. Set the following property in `server.properties`:

```
auth.login.banner=config/loginbanner.txt
```

This property configures the Manager to display the text from the file `<ARCSIGHT_HOME>/config/loginbanner.txt` whenever a user runs the Console. (Changes to the properties file take effect the next time the Manager is started.)

Create a text file named `loginbanner.txt` in the `<ARCSIGHT_HOME>/config` directory. This feature is often used to display a legal disclaimer message. Users must close the message window before they can log in.

The ArcSight Web console will display the custom banner as well, provided that the browser used supports JavaScript and has JavaScript enabled. To configure a custom banner for Web Console:

- 1 Create a custom logo image in .gif or .png format (such as `MyLogo.gif`). The image should be approximately 138 x 39 pixels.
- 2 On the Web server machine, copy this custom logo image file to the `<ARCSIGHT_HOME>/webapp/images` directory.
- 3 Copy the following properties from the `example.styles.properties` file located at `<ARCSIGHT_HOME>/config/web` directory to `styles.properties` file in the same directory. Create a `styles.properties` file if one does not already exist.

```
# logo image for login page
loginLogoImg = <demo-logo-login.png>
```

- 4 Replace 'demo-logo-login.png' with your custom logo image file name. For example, `loginLogoImg=MyLogo.gif`
- 5 Close the Web Console.
- 6 Restart Web server and log into the Web console.

You should see this newly added custom Web logo image in Web console Login Window.



**Caution**

When you uninstall the Web, `style.properties` and your custom logo image files are deleted. Make sure to save these files so that you can use them when you reinstall the Web

## Starting ArcSight SmartConnectors

Before you start ArcSight SmartConnectors, make sure ArcSight Manager is running. It's also a good idea for the ArcSight Console to also be running, so that you can see the status of the configured SmartConnectors and view messages as they appear on the Console. To start up an ArcSight SmartConnector:

- 1 Open a command window or terminal box.
- 2 Type in the following line and press **Enter**:

```
./arcsight agents
```

## Stopping the ArcSight Manager

When not running as a service, press **Ctrl-C** in the command window or terminal box where the ArcSight Manager is running to initiate a controlled shutdown of ArcSight Manager.



Closing the command prompt or terminal box will shut down the ArcSight Manager.

---

## Reconnecting to the ArcSight Manager

If the ArcSight Console loses its connection to the ArcSight Manager—because the Manager was restarted, for example—a dialog box appears in the ArcSight Console stating that your connection to the ArcSight Manager has been lost. Click **Retry** to re-establish a connection to the ArcSight Manager or click **Relogin**.



The connection to the ArcSight Manager cannot be re-established while the ArcSight Manager is restarting. In some cases, a connection cannot be established without resetting one or both machines.

Clicking **Retry** may display connection exceptions while the ArcSight Manager is restarting, or as the connection is re-established.

---

## Configuring ArcSight Manager or ArcSight Web as a Service

The ArcSight Manager (or ArcSight Web) can be configured as a Windows Service or Unix daemon. When you start the ArcSight Manager as a service (or daemon) you can monitor whether or not it has successfully started by viewing the `server.std.log` file located in `<ARCSIGHT_HOME>/logs/default`.

### ArcSight Manager Service Setup on Windows

If the ArcSight Manager was not originally configured as a service, you can do so at any time using the Manager service tool, `managersvc`. To set up ArcSight Manager as a service in Windows:

From a command window in the `<ARCSIGHT_HOME>\bin` directory, enter the following command:

```
arcsight managersvc -i
```

On a 64-bit machine enter:

```
arcsight managersvc64 -i
```

### Starting and Stopping the ArcSight Manager Service on Windows

To start or stop the ArcSight Manager service:

- 1 Right-click the **My Computer** icon, and select **Manage**. The Computer Management window appears.
- 2 Within the Computer Management window, expand the Services and Applications folder.

- 3 Click **Services**.
- 4 Right-click the ArcSight Manager service name and select **Start to begin the service** or **Stop to end the service**

## Removing the ArcSight Manager Service on Windows

Stopping the ArcSight Manager service does not remove it from your system. To remove the service you must do the following:

Within a Windows command prompt, type in the following command from the `<ARCSIGHT_HOME>\bin` directory:

```
arcsight managersvc -r
```

On 64-bit machine enter:

```
arcsight managersvc64 -r
```

Check to ensure that the service was removed. If it was not, reboot the Windows system to completely remove the service.

Doing an uninstall should automatically remove the service too. For the Manager service to start automatically at system boot the option for it must be selected in the Manager setup.

## ArcSight Manager or ArcSight Web Service Setup on Unix Platforms

The following provides a brief overview of how to set up ArcSight Manager or ArcSight Web as a daemon, the “service” equivalent on Unix platform machines. After installation, ArcSight Manager can be controlled using `/etc/init.d/arcsight_manager start|stop`, (or `arcsight_web` for ArcSight Web) following the standard method of starting daemon services in Unix. Change the configuration file `/etc/arcsight/arcsight_manager.conf` (or `arcsight_web.conf` for ArcSight Web) to reflect the installation directory and other settings. In addition, the `/etc/init.d/arcsight_*` scripts will be hooked into the Unix startup procedure, making the ArcSight Manager or Web start and shut down in lock step with the host OS.

To set up ArcSight Manager or ArcSight Web as a Unix daemon, open a terminal box on `<ARCSIGHT_HOME>/bin` and run the appropriate wizard:

```
./arcsight managersetup
```

```
./arcsight websetup
```

Once everything is configured properly, test your configuration setup the next time you start the ArcSight Manager using `/etc/init.d/arcsight_manager` (or `arcsight_web`).

Make sure to start ArcSight Manager this way at least once before relying on it to start correctly during system boot or startup.



The script output will go to `<ARCSIGHT_HOME>/logs/default/server.script.log`. The stdout output of the ArcSight Manager will go to `<ARCSIGHT_HOME>/logs/default/server.std.log`. ArcSight recommends that you tail these two files to identify the cause of any startup failures.

## Reducing Impact of Anti-Virus Scanning

Files in certain ArcSight ESM directories are updated frequently; for example, the log directory. When an anti-virus application monitors these directories, it can impact the system in these ways:

- Place a large and constant load on the CPU of the machine.
- Slow down ArcSight ESM as frequent scanning can impede writes to disk.

Therefore, we recommend that you exclude the following directories (and any subdirectories under them) in `<ARCSIGHT_HOME>` from the virus scan list:

- `caches/server`
- `logs`
- `system`
- `tmp`
- `user`, but include the `user/agent/lib` directory in the scan
- `archive`

## License Tracking and Auditing

ESM appliance automatically maintains a license audit history that allows you to see how many licenses are currently in use. When users log into the Console they will receive a warning notifying them if they have exceeded their current license. An internal audit event will be created for each licensable component to help users track which areas have been exceeded. There are licensing reports on individual features. These reports are located in `/All Reports/ArcSight Administration/ESM/Licensing/`. The reports provide a summary for the number of Actors, Assets, Users, Devices, and EPS identified over the last week.

## Licensed EPS Compliance

By default, your events per second (EPS) throughput is monitored once every 24 hours and an average EPS value is calculated for that period. Your license places a limit on this average EPS throughput. It also places a limit on the number of times you are allowed to exceed the EPS limit over a period (rolling window) of days. In a given window, each time your EPS throughput exceeds the limit allowed by your license, it gets recorded. As soon as you cross the number of times permitted by your license to exceed the EPS limit, your installation becomes noncompliant causing you to be temporarily locked out from using certain functionality (for example, some Console features might get disabled).

An Example:

Say your license is set up for the following:

- Number of incoming EPS allowed = 1000 EPS
- Number of times allowed to exceed 1000 EPS = 5 times
- Period over which you are allowed to exceed the 1000 EPS limit 5 times = 7 days

The above three bullets indicate that on any given day, as long as you have not exceeded an average of 1000 EPS more than 5 times in the past 7 days (counting today as day 1), you are in compliance with your license. But, if you exceed the 1000 EPS limit for the 6th time within the past 7 days, you become noncompliant and may lose some functionality as a consequence.

Once the functionality gets disabled, it stays disabled for a period of time. The length of this period starts with one hour and progressively increases by an hour for each consecutive day that the system is noncompliant. It can increase up to a maximum of 5 hours depending upon how long you have been noncompliant. So, suppose your license allows you to exceed the EPS limit 5 times in a 7-day period, when you exceed the limit a 6th time in the same period, your functionality will be disabled for an hour. If you exceed the limit for a 7th time in the same period it will be disabled for 2 hours, 8th time for 3 hours, and so on until you hit a maximum of 5 hours which is the maximum penalty time. Thereafter, each time you exceed the limit, you will be locked out for 5 hours.

As days go by, if you reach the EPS limit violation of 5 times or less in the past 7 consecutive days, you become compliant and the features that were disabled automatically get enabled.





## Chapter 2

# Configuration

---

This chapter describes the various tasks that you can perform to manage the component configuration. The following topics are covered in this chapter:

- [“Managing and Changing Properties File Settings” on page 17](#)
- [“Adjusting Console Memory” on page 22](#)
- [“Adjusting Pattern Discovery Memory” on page 23](#)
- [“Installing New License Files Obtained from ArcSight” on page 23](#)
- [“Configuring ArcSight Manager Logging” on page 24](#)
- [“Understanding SSL Authentication” on page 34](#)
- [“Reconfiguring the ArcSight Console after Installation” on page 75](#)
- [“Reconfiguring ArcSight Manager” on page 75](#)
- [“Manager Password Configuration” on page 76](#)
- [“Compression and Turbo Modes” on page 84](#)
- [“Configuring the ArcSight Database Monitor” on page 85](#)
- [“Sending Events as SNMP Traps” on page 86](#)

## Managing and Changing Properties File Settings

Various components of ESM use properties files for configuration. Many sections of this documentation require you to change properties in those files. Some of the properties files are also modified when you use one of the configuration wizards that come with ESM.

### Property File Format

Generally, all properties files are text files containing pairs of keys and values. The keys determine which setting is configured and the value determines the configuration value. For example, the following property configures the port on which ArcSight Manager listens:

```
servletcontainer.jetty311.encrypted.port=8443
```

Blank lines in this file are ignored as well as lines that start with a pound sign ( # ). Lines that start with a pound sign are used for comments.

### Defaults and User Properties

Most configuration items in various components consist of at least two files. The first, generally referred to as the defaults properties file, contains the default settings that ESM

provides. These files should never be modified, but can be used as a reference. Updates to the components will overwrite this file to include new settings.

The second file, generally referred to as the user properties file, contains settings that are specific to a particular installation. Settings in the user properties file override settings in the defaults properties file. Typically, the user properties file for a component is created and modified automatically when you configure the component using its configuration wizard. Because the user properties file contains settings you specify to suit your environment, it is never replaced by an upgrade.

The following table lists the most important properties files.

Default Properties	User Properties	Purpose
<code>config/ server.defaults.properties</code>	<code>config/server.properties</code>	ArcSight Manager Configuration
<code>config/ console.defaults.properties</code>	<code>config/console.properties</code>	ArcSight Console Configuration
<code>config/ client.defaults.properties</code>	<code>config/client.properties</code>	ArcSight Common Client Config
<code>config/agent/ agent.defaults.properties</code>	<code>user/agent/agent.properties</code>	SmartConnector Configuration

## Editing Properties

You can edit the properties using a regular text editor, for example vi or emacs on Unix platforms or MS Notepad on Windows.

If you configured the Console and SmartConnectors using default settings in the configuration wizard, a user properties file is not created automatically for that component. If you need to override a setting on such a component, use a text editor to create this file in the directory specified in the above table.

When you edit a property on a component, you must restart the component for the new values to take effect except for the Manager properties listed in the next section.

If you change a communication port, be sure to change both sides of the connection. For example, if you configure a Manager to listen to a different port than 8443, be sure to configure all the Manager's clients (Consoles, SmartConnectors, ArcSight Web, and so on) to use the new port as well.

Protocol	Port	Configuration
TCP	8443	ArcSight Console to ArcSight Manager communication
TCP	8443	ArcSight SmartConnector to ArcSight Manager communication
TCP	9443	ArcSight Web
	9090	ESM Service Layer Container Port
TCP	1521	ArcSight Manager to ArcSight Database (Oracle communication)

Protocol	Port	Configuration
TCP	389	ArcSight Manager to LDAP server (w/o SSL if enabled)*
TCP	636	ArcSight Manager to LDAP server (w/ SSL if enabled)*
TCP	25	ArcSight Manager to SMTP server (for Notifications)
TCP	110	ArcSight Manager to POP3 server (for Notifications)
TCP	143	ArcSight Manager to IMAP server (for Notifications)
UDP	1645 or 1812	ArcSight Manager to RADIUS server (if enabled)
UDP/TCP	53	ArcSight Console to DNS Server communication (nslookup tool)
UDP/TCP	43	ArcSight Console to Whois Server communication (whois tool)
ICMP	none	ArcSight Console to Target communication (ping tool)

## Dynamic Properties

When you change the following properties in the `server.properties` file on the Manager, you do not need to restart the Manager for the changes to take effect:

- `auth.auto.reenable.time`
- `auth.enforce.single.sessions.console`
- `auth.enforce.single.sessions.web`
- `auth.failed.max`
- `auth.password.age`
- `auth.password.age.exclude`
- `auth.password.different.min`
- `auth.password.length.max`
- `auth.password.length.min`
- `auth.password.letters.max`
- `auth.password.letters.min`
- `auth.password.maxconsecutive`
- `auth.password.maxoldsubstring`
- `auth.password.numbers.max`
- `auth.password.numbers.min`
- `auth.password.others.max`
- `auth.password.others.min`
- `auth.password.regex.match`
- `auth.password.regex.reject`
- `auth.password.unique`
- `auth.password.userid.allowed`
- `auth.password.whitespace.max`
- `auth.password.whitespace.min`
- `external.export.interval`

- `process.execute.direct`
- `servletcontainer.jetty311.log`
- `servletcontainer.jetty311.socket.https.expirationwarn.days`
- `ssl.debug`
- `web.accept.ips`
- `whine.notify.emails`
- `xmlrpc.accept.ips`

After you make the change, you use the `manager-reload-config` command to load those changes to the Manager. Every time the `manager-reload-config` command is successful, a copy of the `server.properties` file it loaded is placed in `<ARCSIGHT_HOME>/config/history` for backup purposes. The `server.properties` file in `<ARCSIGHT_HOME>/config/history` is suffixed with a timestamp and does not overwrite the existing versions, as described in the following example.

## Example

Manager M1 starts successfully for the first time on September 27, 2010, at 2:45 p.m. A backup copy of its `server.properties` file is written to `<ARCSIGHT_HOME>/config/history` with this timestamp:

```
server.properties.2010_09_27_14_45_27_718
```

On September 28, 2010, the M1 administrator adds the following property to the `server.properties` file:

```
notification.aggregation.max_notifications=150
```

When the administrator runs the `manager-reload-config` command at 1:05 p.m. the same day, it runs successfully because this property can be loaded dynamically.

As soon as the updated `server.properties` file is loaded in M1's memory, a backup copy of the updated `server.properties` file is written to `<ARCSIGHT_HOME>/config/history` with appropriate timestamp.

Now, `<ARCSIGHT_HOME>/config/history` contains these two backup files:

```
server.properties.2010_09_27_14_45_27_718
```

```
server.properties.2010_09_28_01_05_40_615
```

On September 29, 2010, the M1 administrator adds this property to the `server.properties` file:

```
notification.aggregation.time_window=2d
```

As this property can be also loaded dynamically, similar to the previous change, once the updated `server.properties` is loaded in M1's memory, a backup copy of the `server.properties` file is written to `<ARCSIGHT_HOME>/config/history` with appropriate timestamp.

Now, `<ARCSIGHT_HOME>/config/history` contains these three backup files:

```
server.properties.2010_09_27_14_45_27_718
```

```
server.properties.2010_09_28_01_05_40_615
```

```
server.properties.2010_09_29_03_25_45_312
```

On September 30, 2010, the M1 administrator updates the `whine.notify.emails` property in the `server.properties` file. When he runs the `manager-reload-config` command, the command fails because this property cannot be loaded dynamically. As a result, these things happen:

- The updated `server.properties` file is not loaded into M1's memory, however, changes made to it are not reverted.
- M1 continues to use the properties that were loaded on September 29th.
- No backup copy is made. The `<ARCSIGHT_HOME>/config/history` directory continues to contain the same three backup files:

```
server.properties.2010_09_27_14_45_27_718
```

```
server.properties.2010_09_28_01_05_40_615
```

```
server.properties.2010_09_29_03_25_45_312
```

The changes made on September 30th will not be effective until M1 is restarted.

## Changing Manager Properties Dynamically

To change any of the properties listed previously, do these steps:

- 1 Change the property in the `server.properties` file and save the file.
- 2 **(Optional)** Use the `-diff` option of the `manager-reload-config` command to view the difference between the server properties the Manager is currently using and the properties that will be loaded after you run this command:

```
arcsight manager-reload-config -diff
```



The `-diff` option compares all server properties—default and user properties. For all options available with the `manager-reload-config` command, see [Appendix A, ArcSight Commands](#), on page 99.

- 3 Run this command in `<ARCSIGHT_HOME>/bin` to load the new values for the properties you changed:

```
arcsight manager-reload-config
```

If this command fails with a warning, it indicates that you are changing properties that require a Manager restart before those changes can take effect. When you get such a warning none of the property changes, including the ones that can be reloaded without restarting the Manager, are applied. You can do one of the following in this situation:

- Revert changes to properties that cannot be loaded without restarting the Manager and rerun the `arcsight manager-reload-config` command.
- Force an update of all properties using the `-as` option, as follows:

```
arcsight manager-reload-config -as
```

When you use the `-as` option, the properties that can be changed without restarting the Manager take effect immediately. The properties that require a Manager restart are updated in the `server.properties` but are not effective until the Manager is restarted.

For example, if you change `auth.password.length.min` to 7 and `search.enabled` to false, you will get the above warning because only `auth.password.length.min` can be updated without restarting the Manager. If you force an update of the `server.properties` file,

`auth.password.length.min` will be set to 7, but `search.enabled` will continue to be set to true until the Manager is restarted.

**Note**

Be careful in using the `-as` option to force reload properties. If an invalid static change is made, it may prevent the Manager from starting up once it reboots.

---

## Changing the Service Layer Container Port

By default the service layer container port is 9090. You can change this port :

- 1 Modifying the following files located in the Manager's `<ARCSIGHT_HOME>`:

- ◆ `/arcsight-dm`  
`/plugins/com.arcsight.dm.plugins.tomcatServer_1.0.0/conf/server.xml`.
- ◆ `/config/proxy.rule.xml`
- ◆ `/config/rewriteProxy.rule.xml`

Make sure to replace the references to port 9090 with an unused port number.

- 2 Restart the Manager.

## Securing the ArcSight Manager Properties File

The ArcSight Manager's `server.properties` file contains sensitive information such as database passwords, keystore passwords, and so on. Someone accessing the information in this file can do a number of things, such as tampering with the database and acting as a pseudo ArcSight Manager. As a result, the `server.properties` file must be protected so that only the user account under which the ArcSight Manager is running is able to read it. This can be accomplished by issuing a `chmod` command in Unix and Linux, for example:

```
chmod 600 server.properties
```

This operation is performed during the ArcSight Manager installation. As a result, only the owner of the file (which must be the user that runs the ArcSight Manager) may read or write to the file. For all other users, access to the file is denied.

**Note**

You can also protect the `server.properties` file on Windows systems with an NTFS file system using Microsoft Windows Access Control Lists (ACLs).

---

## Adjusting Console Memory

Because the ArcSight Console can open up to ten independent event-viewing channels, out-of-memory errors may occur. If such errors occur, or if you simply anticipate using numerous channels for operations or analysis, please make the following change to each affected Console installation.

In the `bin/scripts` directory, in the `console.bat` (Windows) or `console.sh` (Unix) configuration files, edit the memory usage range for the Java Virtual Machine.

## Adjusting Pattern Discovery Memory

By default, Pattern Discovery limits its memory usage to about 4 GB of memory. However, if the search for patterns involves too many transactions and events, the task can run out of memory and abort. You can control the memory limit indirectly by changing the maximum number of transactions and events the Pattern Discovery task can hold in memory. The settings for these values are in the `server.defaults.properties` file in the `config` folder.

- `patterns.transactionbase.max` — The maximum number of transactions allowed in memory. If you exceed this number, these transactions are stored as page file. The default is 10000.
- `patterns.maxSupporterCost` — The maximum number of supporters allowed in memory. If you exceed this number, the pattern discovery task aborts. The default is 80000.
- `patterns.maxUniqueEvents` — The maximum number of unique events allowed in memory. If you exceed this number, the pattern discovery task aborts. The default is 20000.

If the pattern discovery task aborts, a message to that effect appears in the console. Run the pattern discovery task again after increasing the pattern discovery memory usage limits. You can increase the memory usage limit by increasing the three values proportionally. For example, to add 25 percent more memory capacity, you would change the values to:

- `patterns.transactionbase.max=12500`
- `patterns.maxSupporterCost=100000`
- `patterns.maxUniqueEvents=25000`

You can edit the properties file using a regular text editor. After changing any of these values, restart the manager for them to take effect.

## Installing New License Files Obtained from ArcSight

To change the license file you obtained from ArcSight, please follow the steps below:



You will receive new license files packaged as `.zip` files and sent via e-mail from ArcSight.

- 1 On the system where ArcSight Manager is installed, copy the package (`.zip` file) to the `<ARCSIGHT_HOME>` directory (the directory that contains the ArcSight Manager installation).
- 2 Run the following command from the Manager's `/bin` directory:  
`./arcsight deploylicense`
- 3 Restart the Manager.

This wizard replaces the license currently installed with the one included in the file. The Manager detects the new license automatically.

## Installing in Silent Mode

To install the license file in silent mode, you are required to create a properties file and use it. To do so:

- 1 Open a command prompt/shell window.
- 2 From the Manager's `bin` directory, run the following command to open the sample properties file:

```
./arcsight deploylicense -g
```

- 3 Copy and paste the text generated by the command above into a text file.
- 4 Set the following properties:

```
LicenseChoice=1  
  
LicenseFile.filename=<name_of_the_license_zip_file>  
  
replaceLicenseQuestion =yes
```

- 5 Save this text file as `properties.txt` in the Manager's `<ARCSIGHT_HOME>`.
- 6 From the Manager's `bin` directory, run:

```
./arcsight deploylicense -f properties.txt -i silent
```

## Configuring ArcSight Manager Logging

ArcSight Manager outputs various types of information to log files. By default, the logs are located in:

```
<ARCSIGHT_HOME>/logs/default/
```

Various ArcSight Manager utilities write logging information to different sets of log files. Each of those sets can consist of multiple files.

The number and size of the log files are configurable, a typical setting is 10 files with 10 megabytes each. When a log file reaches a maximum size, it is copied over to a different location. Depending on your system load, you may have to change the default settings. To make changes to the logging configuration, change the log channel parameters. The default log channel is called *file*.

For the main ArcSight Manager log file, called `server.log`, the following `server.properties` settings are used:

```
# Maximum size of a log file.  
  
log.channel.file.property.maxsize=10MB  
  
# Maximum number of roll over files.  
  
log.channel.file.property.maxbackupindex=10
```

The first setting affects the size of each individual log file; the second setting affects the number of log files created. The log file currently in use is always the log file with no number appended to the name. The log file with the largest number in its extension is always the oldest log file. All of the log files are written to the `<ARCSIGHT_HOME>/logs/default` directory.



ArcSight Manager and its related tools write the following log files:

Log File	Description
<code>server.log*</code>	The main ArcSight Manager log.
<code>server.status.log*</code>	System status information, such as memory usage etc.
<code>server.channel.log*</code>	Active Channel logs.
<code>server.std.log*</code>	All output that ArcSight Manager prints on the console (if run in command line mode)
<code>server.pulse.log*</code>	ArcSight Manager writes a line to this set of logs every ten seconds. Used to detect service interruptions.
<code>server.sql.log*</code>	If database tracing is enabled, the SQL statements are written to this set of log files.
<code>execproc.log*</code>	Log information about externally executed processes (only on some platforms)
<code>serverwizard.log*</code>	Logging information from the arcsight managersetup utility.
<code>dbwizard.log*</code>	Logging information from the arcsight database init utility.
<code>archive.log*</code>	Logging information from the arcsight archive utility.

## Sending logs and diagnostic information to ArcSight

ArcSight Customer Support may request log files and other diagnostic information to troubleshoot problems. The Send Logs utility automatically locates the log files and compresses them. You will need to send the compressed files to the ArcSight Customer Support server.

- You can run this utility as a wizard directly from the Console interface (GUI) in addition to the command-line interface of each component.
- Optionally, gather diagnostic information such as session wait times, thread dumps, and database alert logs about your ArcSight system, which helps ArcSight Customer Support analyze performance issues on your ArcSight components.



**Note**

You can also use the `arcdt` command to run specific diagnostic utilities from the Manager command line. For more information, see [Appendix A, ArcSight Commands](#), on page 99.

- When you run this utility from the Console, Manager, or Web, you can gather logs and diagnostic information for all components of the system.

## Guidelines for using the Send Logs utility

Keep these guidelines in mind when using the Send Logs utility:

- You can be connected as any valid user on an ArcSight component to collect its local logs; however, you must have administrator access to collect logs from other components. For example, if you are connected as user 'joe' to the Console, you can collect its logs. But if you need to collect logs for the Manager and the database, you must connect to the Console as the ArcSight administrator.
- SmartConnectors must be running version 4037 or later to remotely (using a Console or the Manager) collect logs from them.

- You can only collect local logs on SmartConnectors or ArcSight Database. That is, if you run the Send Logs utility on ArcSight Database, only the database log files are gathered.
- You can run the Send Logs utility on a component that is down. That is, if the ArcSight Database is down, you can still collect its logs using this utility.

If the Manager is down, you can only collect its local logs. However, if you need to collect the database logs as well, use the `arcdt` command on the Manager. For more information, see [Appendix A, ArcSight Commands, on page 99](#).
- All log files for a component are gathered and compressed. That is, you cannot select a subset of log files that the utility should process.
- The Send Logs utility generates a compressed file on your local system that you can send to ArcSight Customer Support by e-mail.
- You can review the compressed file to ensure that only a desired and appropriate amount of information is sent to ArcSight support.
- You can remove or sanitize information such as IP addresses, host names, and e-mail addresses from the log files before compressing them. The options are:
  - ◆ Send log as generated

This option, the default, does not remove any information from the logs files.
  - ◆ Only remove IP address

This option removes IP addresses, but not host names or e-mail addresses, from the logs files.
  - ◆ Remove IP address, host names, e-mail addresses

This option removes all IP addresses and enables you to specify a list of host-name suffixes for which all host names and e-mail addresses will be removed from the logs.

For example, if you specify '[company.com](#)' as a host-name suffix to remove, the Send Logs utility will remove all references to domains such as '[www.company.com](#)' and e-mail addresses such as '[john@company.com](#)' from the logs.

## Gathering logs and diagnostic information

When you run the Send Logs utility on ArcSight SmartConnectors or ArcSight database, it gathers logs and diagnostic information (if applicable) for only those components. However, when you run this utility on ArcSight Console, Manager, or ArcSight Web, you can gather logs and diagnostic information for all or a selected set of ArcSight components.

To run this utility on SmartConnectors, enter this in `<ARCSIGHT_HOME>/bin`:

```
./arcsight agent sendlogs
```

To gather logs and diagnostic information for all or a selected set of components, do one of the following:

- On the ArcSight Console, click **Tools | SendLogs**.
- Enter this command in `<ARCSIGHT_HOME>/bin` on Console, Manager, or Web:

```
./arcsight sendlogs
```

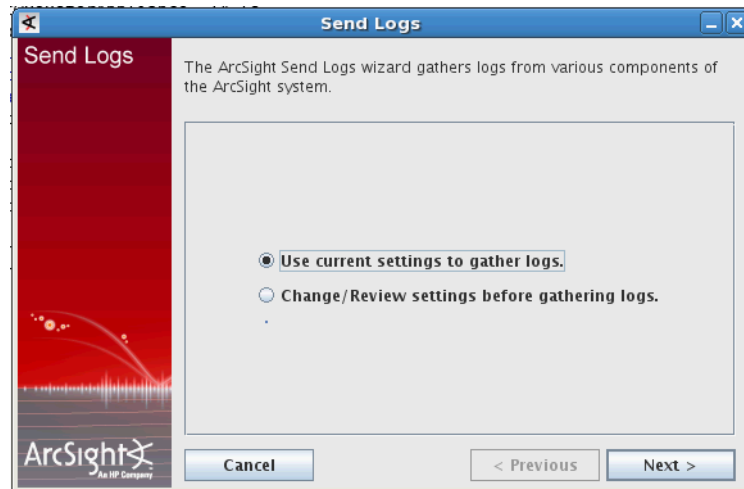
The above action starts the Send Logs wizard. In the wizard screens, perform these steps:



**Note**

The Send Logs wizard remembers most of the choices you make when you run it for the first time. Therefore, for subsequent runs, if you choose to use the previous settings, you will need to enter only some of the following information.

- 1 Decide whether you want the wizard to gather logs only from the component on which you are running it or from all components.



If you select **Use current settings to gather logs.** logs for all components will be gathered thus: If this is the first sendlogs is run after installation, then all the logs are gathered. If this is not the first sendlogs is run, then it will use the same setting as the previous run.

- a You will be asked to enter the Manager's login information.
- b Go to [Step 2 on page 31](#).

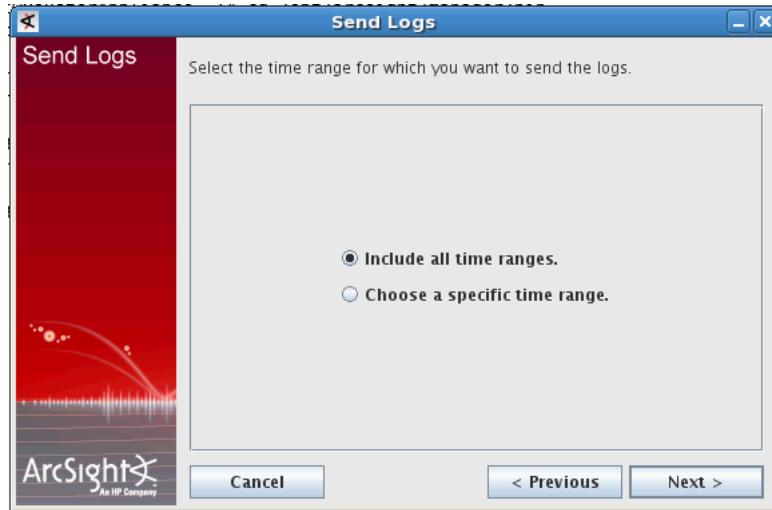
If you selected **Change/Review settings before gathering logs.** you will be provided the option to select the components for which you want logs gathered.

Select whether you want only the local (the component from where you ran the Send Logs utility) logs selected or you want logs from other components collected too.



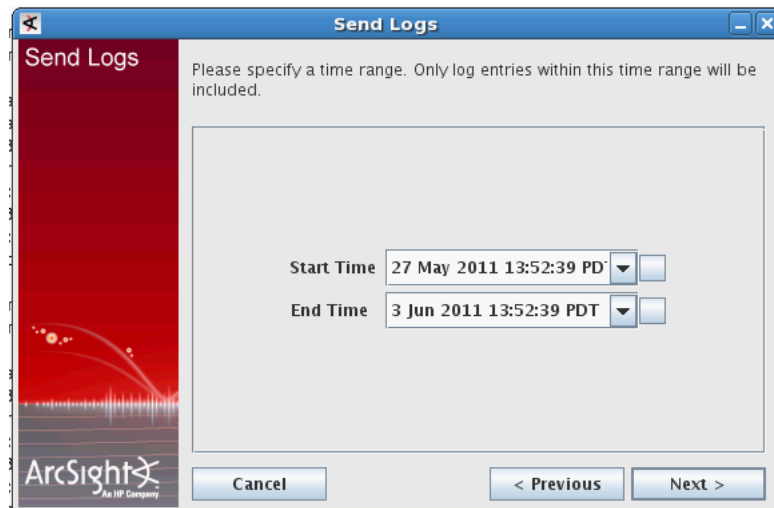
**Local logs only:**

If you selected **Local logs only**, you will be prompted to either choose a time range or include all time ranges.



If you selected **Include all time ranges**, go to [Step 2 on page 31](#).

If you selected **Choose a specific time range**, you will be prompted to enter a start time and end time - a time range for which the wizard will gather the logs.



Go to [Step 2 on page 31](#).

**Logs from other components (Requires Manager credentials):**

If you selected **Logs from other components (Requires Manager credentials)**, you will be prompted to choose the components.

- a Select the components and the time range for which you want to gather logs. In addition, select whether you want to run the diagnostic utilities to gather additional information for those components.



If you choose to specify the diagnostic utilities to run, you will be prompted to select the utilities from a list in a later screen. The diagnostic utilities you can select are:

- ◆ **runsql**—Run SQL commands contained in a file that is specified as a parameter of this utility.

For example, to use the **runsql** utility to find out the number of cases in your ArcSight Database, do the following:

- i Create a file called **sample.txt** in **<ARCSIGHT\_HOME>/temp** on the Manager with this SQL command:

```
select count(*) from arc_resource where resource_type=7;
```

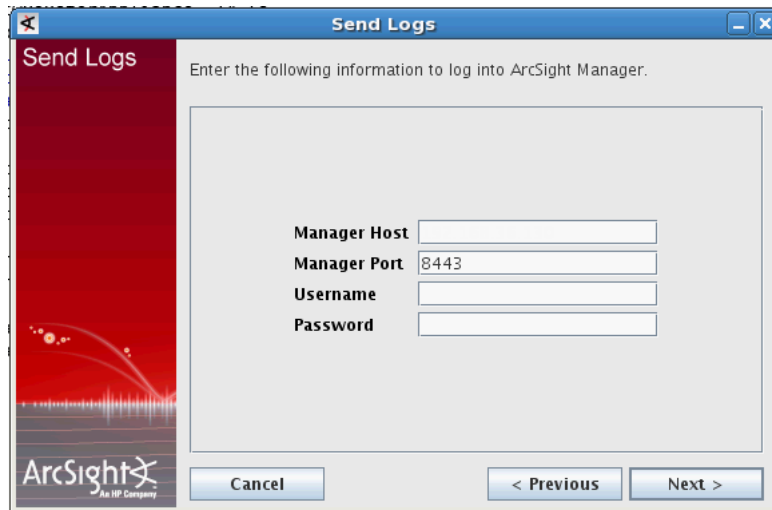
- ii Run this command:

```
arcdt runsql <ARCSIGHT_HOME>/tmp/sample.txt
```

- ◆ **db-alertlog**—Retrieve the database alert log from the database machine.
- ◆ **session-waits**—Retrieve the currently running JDBC (Java Database Connection) sessions and their wait times.
- ◆ **thread-dumps**—Obtain thread dumps from the Manager.

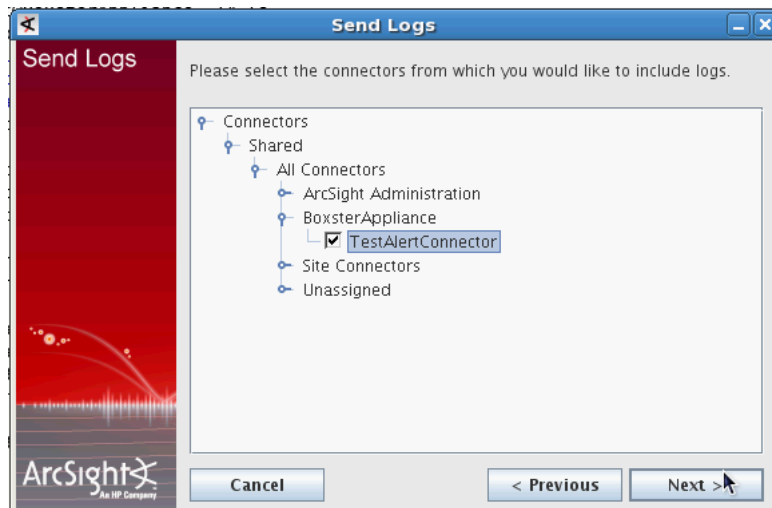
For more details on these commands, see the [Appendix A, arcdt](#), on page 106.

- b Enter information to log in to your ArcSight Manager.



The 'Send Logs' dialog box has a blue title bar and a red sidebar with the ArcSight logo. The main area is light gray and contains the text 'Enter the following information to log into ArcSight Manager.' Below this text are four input fields: 'Manager Host', 'Manager Port' (with '8443' entered), 'Username', and 'Password'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- c If you chose to gather logs from the SmartConnectors, select those SmartConnectors in the next screen.

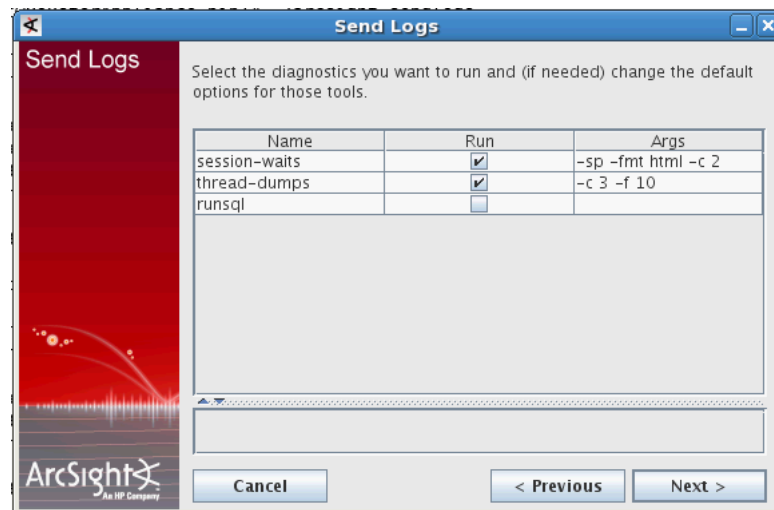


The 'Send Logs' dialog box has a blue title bar and a red sidebar with the ArcSight logo. The main area is light gray and contains the text 'Please select the connectors from which you would like to include logs.' Below this text is a tree view of connectors. The tree structure is: 'Connectors' (expanded) -> 'Shared' (expanded) -> 'All Connectors' (expanded) -> 'ArcSight Administration' (expanded) -> 'BoxsterAppliance' (expanded) -> 'TestAlertConnector' (checked). Other connectors under 'Shared' include 'Site Connectors' and 'Unassigned'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

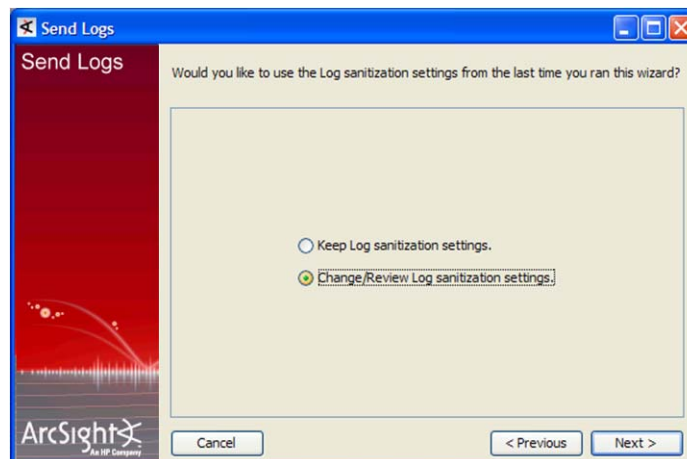


At a minimum, the SmartConnectors should be running version 4037 or later.

- d If you chose to select the diagnostic utilities you want to run earlier in this wizard, select them in the next screen.

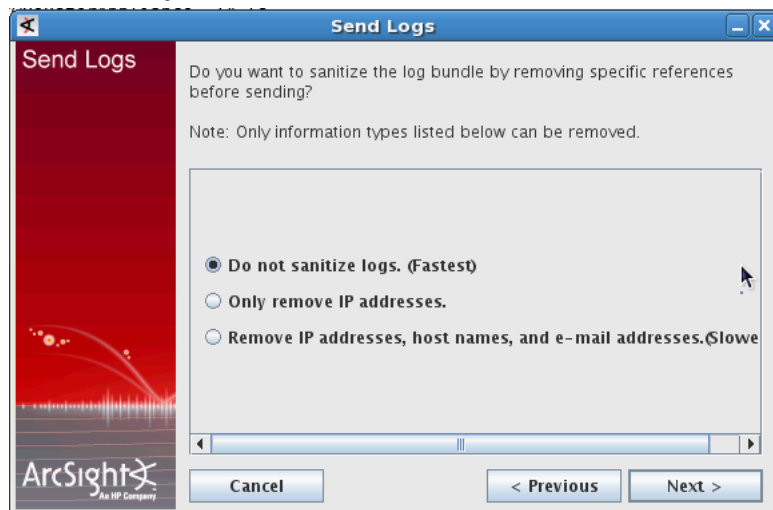


- e Go to [Step 2 on page 31](#).
- 2 Select whether you want to sanitize the logs before sending. For more information about sanitizing options, see [“Guidelines for using the Send Logs utility” on page 25](#).



If you choose **Keep Log sanitization settings**, go to [Step 3 on page 33](#).

If you choose **Change/Review Logs sanitization settings**, you will be prompted to select what you want to sanitize.



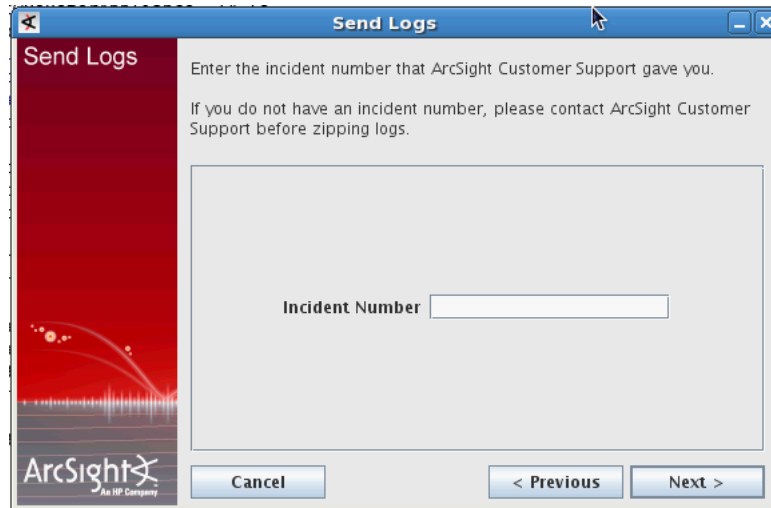
If you chose either option #1 or #2, go to [Step 3 on page 33](#).

If you selected **Remove IP addresses, host names, and e-mail addresses (Slower)**, you will be prompted to enter what you want removed.





3 Enter the ArcSight Support incident number.



The 'Send Logs' dialog box has a blue title bar and a red sidebar with the ArcSight logo. The main area contains the following text:

Enter the incident number that ArcSight Customer Support gave you.  
If you do not have an incident number, please contact ArcSight Customer Support before zipping logs.

Below the text is a large text input field labeled 'Incident Number'.

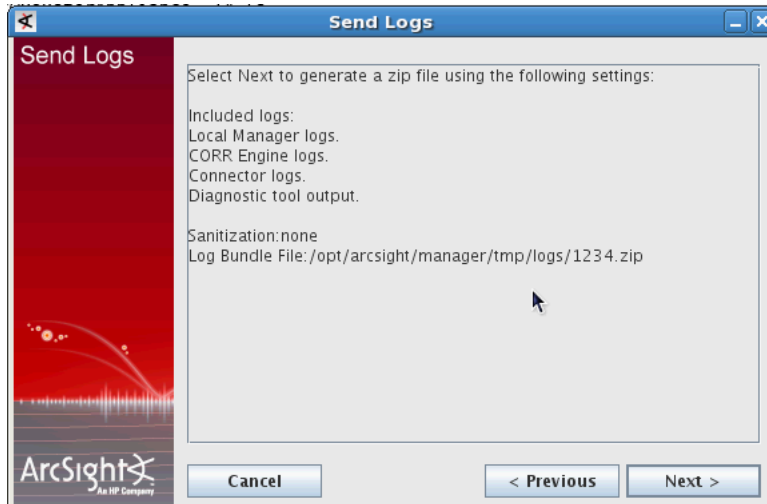
At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

The Send Logs utility uses this number to name the compressed file it creates. Use the incident number that ArcSight Customer Support gave you when you reported the issue for which you are sending the logs. Doing so helps Customer Support easily relate the compressed file to your incident.

In case you do not have an incident number at this time, you can continue by entering a meaningful name for the compressed file to be created and once you obtain the incident number from ArcSight Customer Support, you can rename the file with the incident number you received.

If you have not reported an incident for which you are sending the logs, ArcSight strongly recommends that you do so before packing the logs.

4 Click **Next** to start the compression.



The 'Send Logs' dialog box shows the following settings:

Select Next to generate a zip file using the following settings:

Included logs:  
Local Manager logs.  
CORR Engine logs.  
Connector logs.  
Diagnostic tool output.

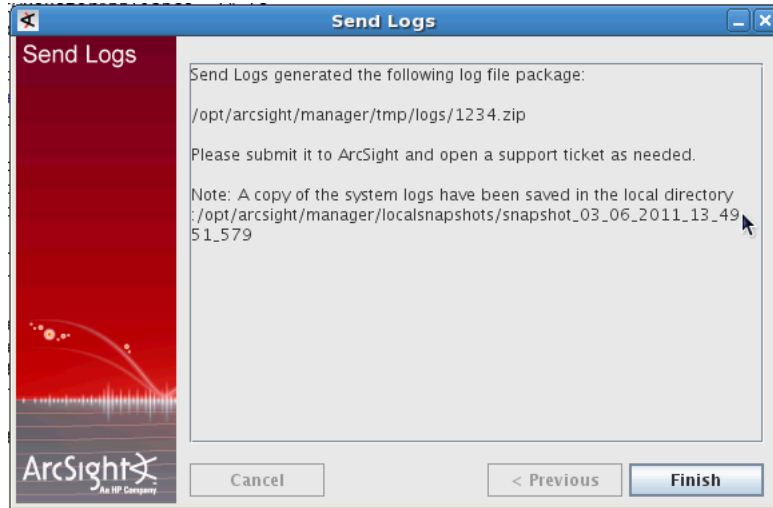
Sanitization: none  
Log Bundle File: /opt/arc sight/manager/tmp/logs/1234.zip

At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.



Most of the values you entered during the first run of the Send Logs wizard are retained. The next time you run this wizard, you need to enter only a few settings.

- 5 Click **Finish** in the last screen.



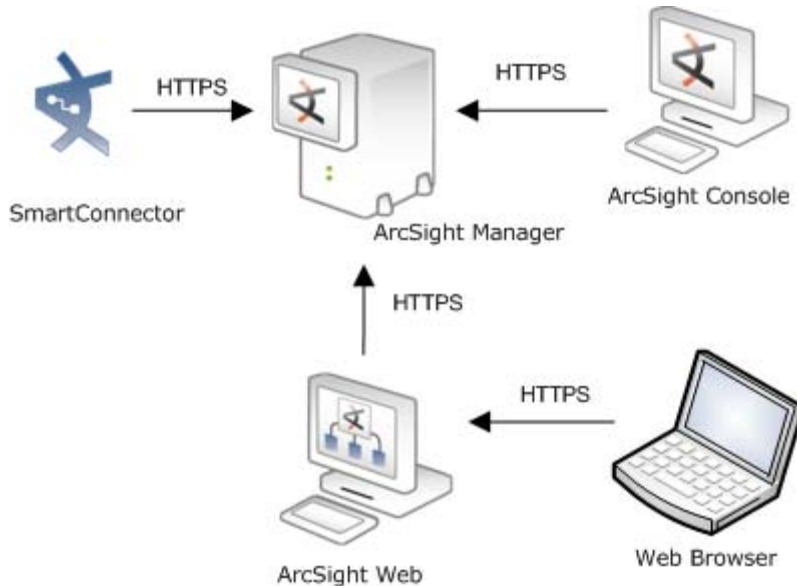
## Understanding SSL Authentication

Secure Socket Layer (SSL) technology is used for communication between ArcSight Manager and its clients—Console, SmartConnectors, and ArcSight Web. SSL is also used between ArcSight Web and the web browsers that communicate with it.

SSL enables the Manager and ArcSight Web (referred to as a "server" from here on) to authenticate to its clients and communicate information over an encrypted channel, thus providing the following benefits:

- Authentication—Ensuring that clients send information to an authentic server and not to a machine pretending to be that server.
- Encryption—Encrypting information sent between the clients and the server.
- Data Integrity—Hashing information to prevent intentional or accidental modification.

By default, clients submit a valid user name and password to authenticate with the server; however, these clients can be configured to use SSL client authentication.



SSL is not used between ArcSight Manager and the ArcSight Database.

## Terminology

These terms are used in describing and configuring SSL:

- Certificate

A certificate contains the public key, identifying information about the machine such as machine name, and the authority that signs the certificate. SSL certificates are defined in the ISO X.509 standard.

- Key pair

A key pair is a combination of a private key and the public key that encrypts and decrypts information. A machine shares only its public key with other machines; the private key is never shared. The public and private keys are used to set up an SSL session. For details, see [“How SSL Works” on page 44](#).



The `keytoolgui` utility, used to perform a number of SSL configuration tasks, refers to a combination of an SSL certificate and private key as the key pair.

The `keytoolgui` utility is discussed in [“Tools for SSL configuration” on page 39](#).

- SSL server-SSL client

An SSL session is set up between two machines—one of them acts as the server and the other as a client. Typically, a server must authenticate to its clients before they will send any data. However, in client-side SSL authentication, the server and its clients authenticate each other before communicating.

ArcSight Manager is an SSL server, while SmartConnectors, Console, and browsers are SSL clients. ArcSight Web is an SSL client to the Manager and an SSL server to the web browsers that connect to it.

#### ■ Key store

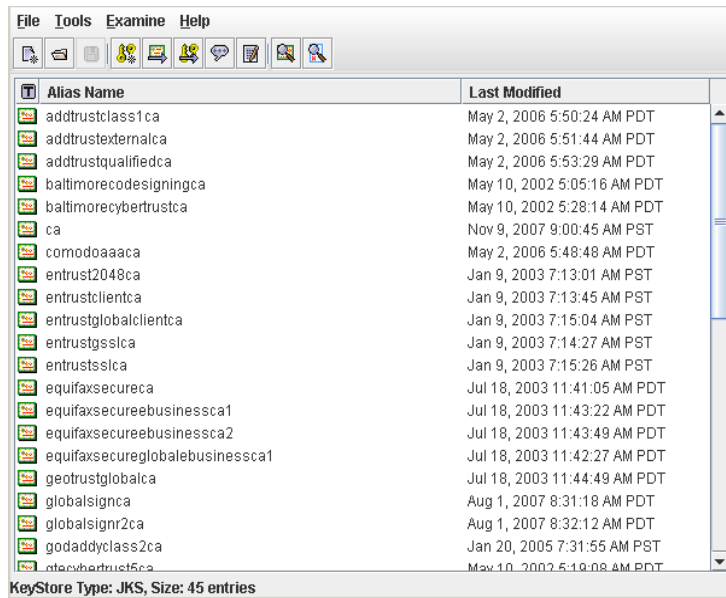
A key store is an encrypted repository on the SSL server that holds the SSL certificate and the server's private key. The following table lists the ArcSight component, the name of the key store on that component, and its location.

Log File	Key Store File Name**	Location of Key Store
Manager	keystore	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webkeystore	<ARCSIGHT_HOME>/config/jetty
Clients* (for client-side authentication)	keystore.client	<ARCSIGHT_HOME>/config

\*When client-side authentication is used, a key store exists on both—the server and the client.

\*\*Make sure you do not change the keystore file name.

#### ■ Trust store



Trust store is an encrypted repository on SSL clients that contains a list of certificates of the issuers that a client trusts.



The [keytoolgui](#) utility, used to view a trust store, is discussed in [“Tools for SSL configuration” on page 39](#).

When an issuer issues a certificate to the server, it signs the certificate with its private key. When the server presents this certificate to the client, the client uses the issuer's public key from the certificate in its trust store to verify the signature. If the signature matches, the client accepts the certificate. For more details, see how SSL handshake occurs in [“How SSL Works” on page 44](#).

The following table lists the ArcSight component, the name of the trust store on that component, and its location.

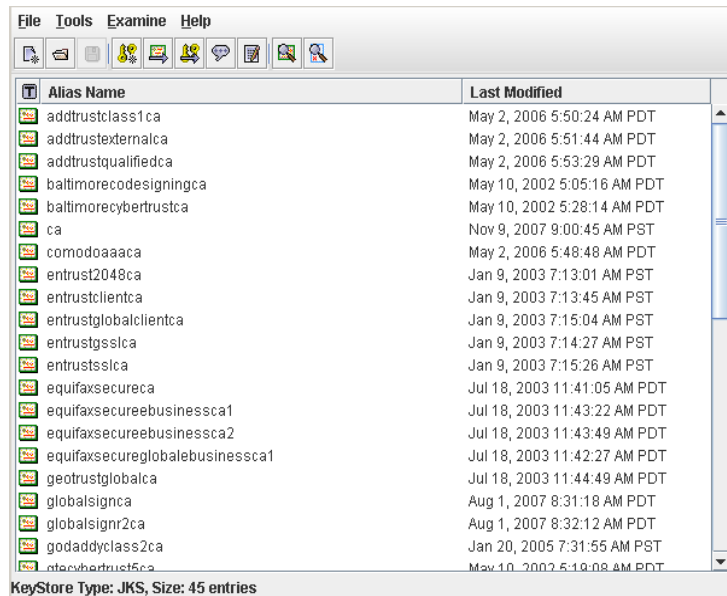
Component	Trust Store File Name	Location of Trust Store
Clients	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	cacerts[1]	<ARCSIGHT_HOME>/jre/lib/security
ArcSight Web	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	truststore[2]	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webtruststore[2][3]	<ARCSIGHT_HOME>/config/jetty

[1] The utilities that exist on the Manager machine such as archive are treated as clients of the Manager. The cacerts file on the Manager is used for authenticating the Manager to these clients.

[2] When client-side authentication is used.

[3] When client-side authentication is used, ArcSight Web contains two trust stores—cacerts for connections to the Manager and webtruststore for connections to browsers.

#### ■ Alias



Certificates and key pairs in a key store or a trust store are identified by an alias.

#### ■ Key store / Trust store password

A key store password is used to encrypt the key store file. Similarly, a trust store password is used to encrypt a trust store file. Without this password, you cannot open these files.

You specify a key store password when creating a key pair, which is discussed in later sections of this chapter. The password is obfuscated and stored in the ArcSight component's `*.properties` file. The following table lists the property file and the property name where the key store password is stored for each component.

A default trust store password is set up for each ArcSight component in its `*.defaults.properties` file. The password is unobfuscated. Typically, you will not need to change this password. However, if you want to change or obfuscate this password, use the `changepassword` utility. For information about `changepassword`, see Appendix A. The following table lists the property name where the obfuscated trust store password is stored.

Password Type	Property File	Property Name
Key Store		
Manager	<code>server.properties</code>	<code>server.privatekey.password.encrypted</code>
ArcSight Web	<code>webserver.properties</code>	<code>server.privatekey.password.encrypted</code>
Client*	<code>client.properties**</code>	<code>ssl.keystore.password.encrypted</code>
Trust Store		
Client	<code>client.properties**</code>	<code>ssl.truststore.password</code>
Manager*	<code>server.properties</code>	<code>servletcontainer.jetty311.truststore.password.encrypted</code>
ArcSight Web	<code>webserver.properties</code>	<code>servletcontainer.jetty311.truststore.password.encrypted</code>

\*For client-side authentication

\*\* If the `client.properties` file does not exist on your client, you will need to create it using an editor of your choice.

#### ■ Cipher suite

A set of authentication, encryption, and data integrity algorithms used for securely exchanging data between an SSL server and a client.

The following cipher suites are enabled by default:

- ◆ TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- ◆ SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- ◆ SSL\_RSA\_WITH\_RC4\_128\_MD5
- ◆ SSL\_RSA\_WITH\_RC4\_128\_SHA

Other supported cipher suites are:

- ◆ TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- ◆ TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- ◆ SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- ◆ SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- ◆ SSL\_RSA\_WITH\_DES\_CBC\_SHA
- ◆ SSL\_DHE\_RSA\_WITH\_DES\_CBC\_SHA
- ◆ SSL\_DHE\_DSS\_WITH\_DES\_CBC\_SHA
- ◆ SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5
- ◆ SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA
- ◆ SSL\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

- ◆ SSL\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA
- ◆ SSL\_RSA\_WITH\_NULL\_MD5
- ◆ SSL\_RSA\_WITH\_NULL\_SHA
- ◆ SSL\_DH\_anon\_WITH\_RC4\_128\_MD5
- ◆ TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA
- ◆ SSL\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA
- ◆ SSL\_DH\_anon\_WITH\_DES\_CBC\_SHA
- ◆ SSL\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5
- ◆ SSL\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA

Although in most cases you do not need to change cipher suites, you can configure them in the properties file for an ArcSight component:

- ◆ Manager—[server.properties](#)
- ◆ Arcsight Web—[webserver.properties](#)
- ◆ Clients—[client.properties](#)

During the SSL handshake, the client provides a list of cipher suites that it can accept, in descending order of preference. The server compares the list with its own set of acceptable cipher suites, picks one to use based on its order of preference, and communicates it to the client.

## Tools for SSL configuration



Not all ESM versions or ArcSight Express models support the FIPS mode. PKCS#11 token support may not be available for all ESM versions and ArcSight Express models.

### Keytoolgui

The [keytoolgui](#) utility enables you to perform a number of SSL configuration tasks. Some of these tasks are:

- Creating a new key store
- Creating a new key pair
- Creating a request for a CA-signed certificate ([.csr](#) file)
- Exporting and Importing a key pair
- Exporting and Importing a certificate

The [keytoolgui](#) utility is available on all components and is located in the [<ARCSIGHT\\_HOME>/bin/scripts](#) directory of the component.



Be sure to have X11 enabled on UNIX to run this tool.

To run [keytoolgui](#), run this command in [<ARCSIGHT\\_HOME>/bin](#):

```
./arcsight keytoolgui
```

On SmartConnectors, use:

```
./arcsight agent keytoolgui
```

### Using Keytoolgui to Export a Key Pair

- 1 Start the keytoolgui by running the following from the Manager's `bin` directory:  

```
./arcsight keytoolgui
```
- 2 Click **File->Open KeyStore** and navigate to the component's keystore.
- 3 Enter the password for the keystore when prompted. The default password is "changeit" (without quotes).
- 4 Right-click the key pair and select **Export**.
- 5 Select **Private Key and Certificates** radio button and click **OK**.
- 6 Enter the password for the key pair when prompted. The default password is "changeit" (without quotes).
- 7 Enter a new password which will be used for the exported key pair file, then re-enter it to confirm it and click **OK**.
- 8 Navigate to the location on your machine to where you want to export the key pair.
- 9 Enter a name for the key pair with a `.pfx` extension in the Filename textbox and click **Export**.
- 10 You will see an Export Successful message.
- 11 Click **OK**.

### Using Keytoolgui to Import a Key Pair

- 1 Start the keytoolgui from the component to which you want to import the key pair. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory:  

```
./arcsight keytoolgui
```
- 2 Select **File->Open KeyStore** and navigate to your component's keystore.
- 3 Enter the key store password when prompted. The default password is "changeit" without the quotes.
- 4 Select **Tools->Import Key Pair** and navigate to the location of the key pair file, select it and click **Choose**.
- 5 Enter the password for the key pair file when prompted and click **OK**.
- 6 Select the key pair and click **Import**.
- 7 Enter an alias for the key pair and click **OK**.
- 8 Enter a new password for the key pair file to be imported, re-enter it to confirm it , and click **OK**.
- 9 You will see a message saying Key Pair Import Successful. Click **OK**.
- 10 Select **File->Save Key Store** to save the changes to the keystore and exit the keytoolgui.

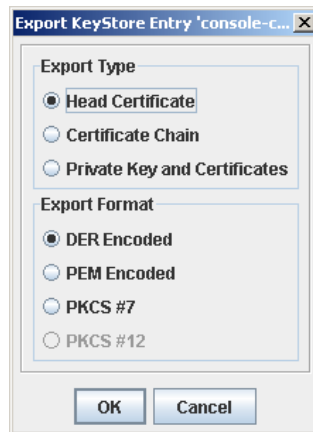
### Using Keytoolgui to Export a Certificate

- 1 Start the keytoolgui from the component from which you want to export the certificate. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory.

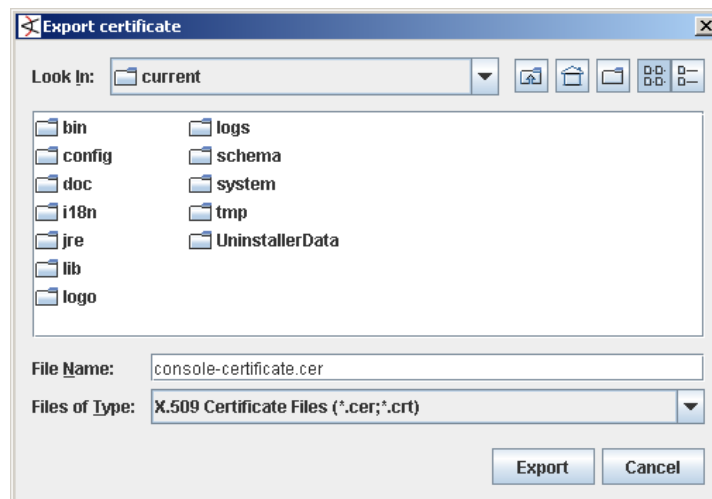


```
./arcsight keytoolgui
```

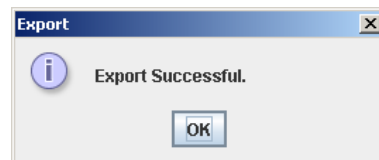
- 2 Select **File->Open KeyStore** and navigate to your component's truststore.
- 3 Enter the truststore password when prompted. The default password is "changeit" without the quotes.
- 4 Right-click the certificate and select **Export**.
- f Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- g Navigate to the location where you want to export the certificate, and enter a name for the certificate with a **.cer** extension and click **Export**.



- h You will see the following message:



- 5 If the component into which you want to import this certificate resides on a different machine than the machine from which you exported the certificate (the current machine), copy this certificate to the to the other machine.

### Using Keytoolgui to Import a Certificate

- 1 Start the keytoolgui from the component into which you want to import the certificate. To do so, run the following command from the component's <ARCSIGHT\_HOME>/bin directory.

```
./arcsight keytoolgui
```

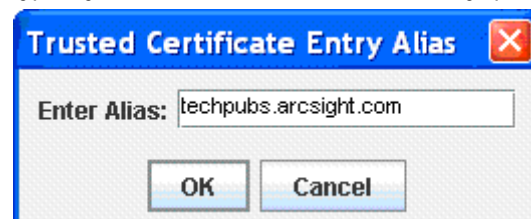
- 2 Click **File->Open Keystore** and navigate to the truststore (<ARCSIGHT\_HOME>/jre/lib/security) of the component.
- 3 Select the store named `cacerts` and click **Open**.
- 4 Enter the password for the truststore when prompted. The default password is 'changeit' (without quotes).
- 5 Click **Tools->Import Trusted Certificate** and navigate to the location of the certificate that you want to import.
- 6 Click **Import**.
- 7 You will see the following message. Click **OK**.



- 8 The Certificate details are displayed. Click **OK**.
- 9 You will see the following message. Click **Yes**.



- 10 Enter an alias for the Trusted Certificate you just imported and click **OK**. Typically, the alias Name is same as the fully qualified host name.



- 11 You will see the following message. Click **OK**.



- 12 Save the trust store file.

### Creating a Keystore Using Keytoolgui

- 1 Start the keytoolgui from the component into which you want to import the certificate. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory.

```
./arcsight keytoolgui
```

- 2 Click **File->New KeyStore**.  
 3 Select **JKS** and click **OK**.  
 4 Click **File->Save KeyStore**.

### Generating a Key Pair Using Keytoolgui

- 1 Start the keytoolgui from the component into which you want to import the certificate. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory.

```
./arcsight keytoolgui
```

- 2 Click **File->Open KeyStore** and navigate to your keystore.  
 3 Click **Tools->Generate Key Pair** and fill in the fields in the General Certificate dialog and click **OK**.  
 4 Enter an alias for the newly created key pair and click **OK**.  
 5 Save the keystore by clicking **File->Save Key Store**.

## keytool

The `keytool` utility is the command-line version of `keytoolgui` that you can use to manipulate the key stores and trust stores directly. To use `keytool`, enter this command:

```
arcsight keytool -store store
```

where `store` can be `managercerts`, `managerkeys`, `clientcerts`, `clientkeys`, `webcerts`, `webkeys`, `ldapcerts`, or `ldapkeys`.

On SmartConnector hosts, use:

```
arcsight agent keytool -store store
```

To see options available for each store, enter:

```
arcsight keytool -store store
```



There are a few restrictions on the contents of a key store or trust store including that the Manager's certificate should have the alias `mykey`.

---

## tempca

The `tempca` utility enables you to manage the SSL certificate in many ways. To see a complete list of parameters available for this utility, enter this in `<ARCSIGHT_HOME>/bin`:

```
./arcsight tempca
```

On SmartConnectors, use:

```
./arcsight agent tempca
```

A few frequently performed operations using this utility are:

- Viewing the type of certificate in use on the Manager:  

```
./arcsight tempca -i
```
- Removing the Demo certificate from the list of trusted certificates:  

```
./arcsight tempca -rc
```

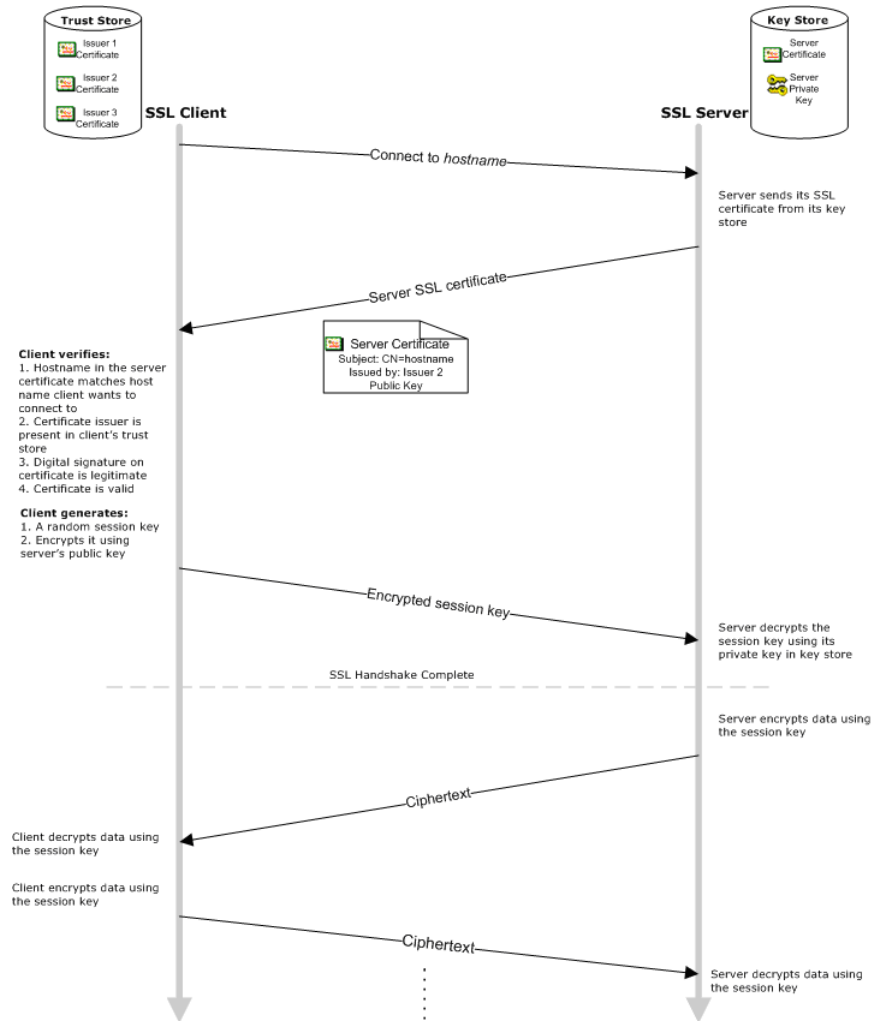
## How SSL Works

When a client initiates communication with the SSL server, the server sends its certificate to authenticate itself to the client. The client validates the certificate by verifying:

- The hostname is identical to the one with which the client initiated communication.
- The certificate issuer is in the list of trusted certificate authorities in the client's trust store (`<ARCSIGHT_HOME>/jre/lib/security/cacerts`) and the client is able to verify the signature on the certificate by using the CA's public key from the certificate in its trust store.
- The current time on the client machine is within the validity range specified in the certificate to ensure that the certificate is valid.

If the certificate is validated, the client generates a random session key, encrypts it using the server's public key, and sends it to the server. The server decrypts the session key using its private key. This session key is used to encrypt and decrypt data exchanged between the server and the client from this point forward.

The next figure illustrates the handshake that occurs between the client and Manager.



**Figure 2-1** SSL handshake between an SSL server and client

If client-side authentication is used, the server requests the client's certificate when it sends its certificate to the client. The client sends its certificate along with the encrypted session key.

## SSL certificates



Note

To replace an expired certificate, you have to delete the old expired certificate from the truststore, cacerts, first and then import the new certificate into cacerts. Since the common name (CN) for the new certificate will be identical to the CN in the old certificate, you are not permitted have both the expired as well as the new certificate co-exist in the cacerts.

To delete a certificate from the truststore, start the keytoolgui and navigate to the certificate, right-click on the certificate and select **Delete**.

Use the keytoolgui to import the new certificate into the truststore or cacerts.



Caution

Not all ESM versions or ArcSight Express models support the FIPS mode.

PKCS#11 token support may not be available for all ESM versions and ArcSight Express models.

### Types

You can use three types of SSL certificates:

- CA-signed
- Self-signed (applicable to default mode only)
- Demo (applicable to default mode only)

CA-signed certificates are issued by a third party you trust. The third party may be a commercial Certificate Authority (CA) such as VeriSign and Thawte or you might have designated your own CA. Because you trust this third party, your clients' trust stores might already be configured to accept its certificate. Therefore, you may not have to do any configuration on the client side. The process to obtain a CA-signed certificate is described in ["Obtaining a CA-signed certificate" on page 52](#).

You can create your own self-signed certificates. A self-signed certificate is signed using the private key from the certificate itself. You will need to configure clients to trust each self-signed certificate you create.

ArcSight includes a built-in "demo" Certificate Authority that can issue a temporary demo certificate during the Manager installation. This CA is provided only to enable you to complete installation in the absence of a signed certificate. However, ArcSight does not recommend using a certificate issued by this CA in production environments. If your Manager was installed with a Demo certificate, you will need to configure your clients to accept this certificate.

### Comparing Self-signed and CA-signed certificates

Self-signed certificates are as secure as CA-signed, however, CA-signed certificates scale better as illustrated in this example:

If you have three SSL servers that use self-signed certificates, you will have to configure your clients to accept certificates from all of them (the three servers are three unique issuers). If you add a new server, you need to configure clients again. However, if these servers use a CA-signed certificate, you need to configure the clients once to accept the certificate. If the number of Managers grows in the future, you do not need to do any additional configuration on the clients.

## Using a Demo Certificate



You can use a demo certificate in default mode only.

To use a demo certificate:

- 1 On the Manager:
  - a Run this command in `<ARCSIGHT_HOME>/bin`:
 

```
./arcsight managersetup
```
  - b In the Manager Configuration Wizard, select **Demo key pair** in the screen that prompts you to select the certificate type.
- 2 On SmartConnectors:
  - a Run this command in `<ARCSIGHT_HOME>/bin`:
 

```
runagentsetup
```
  - b In the SmartConnector Configuration Wizard, select **Yes, the ArcSight Manager is using a demo certificate**.
- 3 On a Console:
  - a Run this command in `<ARCSIGHT_HOME>/bin`:
 

```
consolesetup
```
  - b In the Console Configuration Wizard, select **Yes, the ArcSight Manager is using a demo certificate**.
- 4 On ArcSight Web server:
  - a Run this command in `<ARCSIGHT_HOME>/bin`:
 

```
webserversetup
```
  - b In the Web Configuration Wizard, select **Demo key pair** in the screen that prompts you to select the certificate type.
- 5 On web browsers connecting to ArcSight Web, you do not need to set anything; however, the browsers display a security dialog every time they connect. To stop a browser from displaying this dialog:
  - a In `<ARCSIGHT_HOME>/bin`, run this command on the Manager machine to export the demo CA's certificate:
 

```
arcsight tempca -dc
```

A file named `demo.crt` is created in your current working directory.
  - b Import the `demo.crt` file into your web browser.

See your Web browser's documentation for details.

## Using a Self-Signed Certificate

The procedure you follow depends on the number of ArcSight Managers with which your clients communicate.

### When clients communicate with one ArcSight Manager

To use a self-signed certificate for deployments in which clients communicate with only one ArcSight Manager, perform these steps:

- 1 On the Manager, create a self-signed key pair:

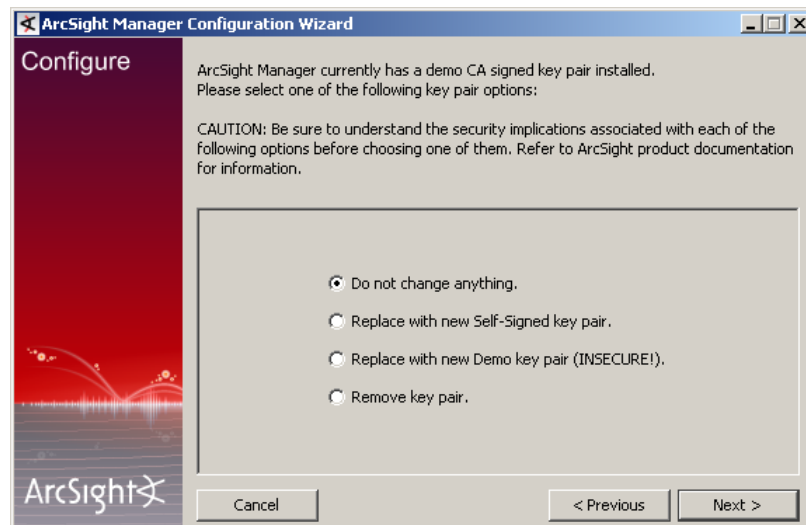


Steps to create a self-signed key pair may be different for a new ArcSight Manager installation as the Configuration Wizard is launched automatically during the installation process.

- a In `<ARCSIGHT_HOME>/bin`, run this command:

```
./arcsight managersetup
```

- b In the Manager Configuration Wizard, select **Replace with new Self-Signed key pair**, and click **Next**.





- c Enter information about the SSL certificate, as shown in this example. Click **Next**.

- d Enter the SSL key store password that will be used for the certificate. Click **Next**.

Remember this password. You will need to use it to open the key store.

- e Step through the Configuration Wizard.

At the end of the Configuration Wizard, these three things happen:

- i The Manager's key store, `<ARCSIGHT_HOME>/config/jetty/keystore`, is replaced with the one created using this procedure.
- ii A `selfsigned.cer` certificate file is generated in the `<ARCSIGHT_HOME>/config/jetty` directory.
- iii The newly generated self-signed certificate is added to the Manager's trust store file, `<ARCSIGHT_HOME>/jre/lib/security/cacerts`.



**Note**

The self-signed certificate does not take effect until the Manager is restarted later in this procedure.



This step overwrites your existing cacerts with the new one that contains the information about the Trusted Certificate Authority (CA) that signed your self-signed certificate. However, the new cacerts file does not take effect until the client is restarted later in this procedure.

- 2 Export the Manager's certificate from `<ARCSIGHT_HOME>/jre/lib/security/cacerts`.
- 3 Make sure to copy the Manager's certificate on the machine on which the clients connecting to the Manager are/will be installed.
- 4 Import the Manager's certificate to the `<ARCSIGHT_HOME>/jre/lib/security` directory on all clients. See ["Using Keytoolgui to Import a Certificate" on page 42](#).



Make sure you have imported the Manager's certificate to all existing clients before proceeding further. Otherwise, after you perform the next steps, only clients with the new Manager's certificate will be able to connect to the Manager.

- 5 Restart the Manager process so that the Manager can start using the self-signed certificate. Restart all clients.
- 6 When installing a new client, repeat Steps 2-4 of this procedure.
- 7 On the ArcSight Web server, perform the steps listed in section ["Setting up SSL Client Authentication on ArcSight Web" on page 65](#).
- 8 On the ArcSight Console, perform the steps listed in section ["Setting up SSL Client-Side Authentication on ArcSight Console running in Default Mode" on page 57](#).

## When clients communicate with multiple ArcSight Managers

To use self-signed certificate for a deployment in which clients communicate with more than one ArcSight Managers, perform these steps for each Manager:

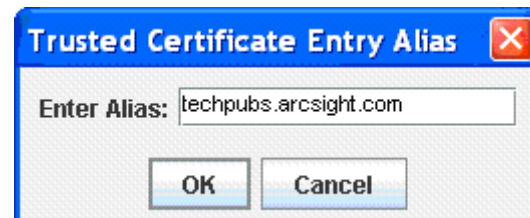


By following this procedure you append the self-signed certificate to the existing client trust store, cacerts. Doing so prevents overwriting cacerts, which happens if you follow the previous procedure.

- 1 Follow Step 1 from the previous procedure on all Managers.
- 2 Copy the selfsigned.cer file from all Managers to the `<ARCSIGHT_HOME>/jre/lib/security` directory on one of your clients.  
  
To prevent a certificate file from overwriting another when you copy multiple certificate files with the same name to the same location, rename each certificate file as you copy. For example, copy the certificate file from ManagerA and rename it to `SelfSigned_MgrA.cer`.
- 3 On that client, use the `keytoolgui` utility to import certificates into the trust store (cacerts):
  - a In `<ARCSIGHT_HOME>/bin`, run this command:  
  
`./arcsight keytoolgui`
  - b Click **File->Open Keystore**.
  - c In `<ARCSIGHT_HOME>/jre/lib/security`, select the store named cacerts. Use the password 'changeit' (without quotes) to open cacerts.

**d** Click **Tools->Import Trusted Certificate:****i** Select the self-signed certificate for a Manager and click **Import**.**ii** You will see the following message. Click **OK**.The Certificate details are displayed. Click **OK**.**iii** You will see the following message. Click **OK**.**iv** Enter an alias for the Trusted Certificate you just imported and click **OK**.

Typically, the alias Name is same as the fully qualified host name.

**v** You will see the following message. Click **OK**.**vi** Save the trust store file.**vii** Repeat Steps i through vi for all self-signed certificates you copied.**e** On the client, enter this command in `<ARCSIGHT_HOME>/bin` to stop the client from using the currently in-use Demo certificate:

```
./arcsight tempca -rc
```

For SmartConnectors, run:

```
./arcsight agent tempca -rc
```

- 4 Copy the `<ARCSIGHT_HOME>/jre/lib/security/cacerts` file from the client in the previous step to all other clients.
- 5 Restart the Manager service so that the Manager can start using the self-signed certificate.
- 6 Restart the client.
- 7 When installing a new client, copy the cacerts file from any client you updated earlier in this procedure.

## Using a CA-Signed Certificate

Obtaining and deploying a CA-signed certificate involves these steps:

- 1 Obtaining a CA-signed certificate.
- 2 Replacing your demo or self-signed certificate with the CA-signed certificate.



Note

You should obtain two CA-signed certificates—one for the Manager and the other for ArcSight Web, unless both components are installed on the same machine. Follow the procedure described in this section to obtain and import the certificates to the Manager, and if appropriate, to ArcSight Web.

---

## Obtaining a CA-signed certificate

To obtain your own CA-signed SSL certificate for ArcSight Manager and ArcSight Web, perform these steps:

- 1 Create a key pair:
  - a On the Manager machine, run this command to launch the `keytoolgui` utility in `<ARCSIGHT_HOME>/bin`:

```
./arcsight keytoolgui
```
  - b Click **File->New KeyStore** to create a new key store.

Make sure to select JKS:

    - JKS (ArcSight default)
    - PKCS #12
  - c To create the key pair, click **Tools->Generate Key Pair**.

Generating the key pair can take some time.

- d Enter information about the new key pair, including the length of time for its validity (in days). Click **OK**.



Note

For Common Name (CN), enter the fully qualified domain name of the Manager. Ensure that DNS servers, which the clients connecting to this host will use, can resolve this host name.

Provide a valid e-mail address as the CAs typically send an e-mail to this address to renew the certificate.

- e Specify an alias called 'mykey' (a name for referring to the new key pair in the future).



Note

The default alias is the Common Name (CN) you provided in the previous step.

- f Click **File->Save** to save the key store.

Save the key store with a name such as `keystore.request`.

If saving the key store on ArcSight Web, save the file with a name such as `webkeystore.request`.

Use the password of your existing key store to save this key store. If you do not remember the password, run the Manager Configuration Wizard and change the password of your existing key store first.

## 2 Create a certificate signing request (CSR):

- a In the `keytoolgui` utility, right-click the new key pair you created (`mykey`) and select **Generate CSR** to create a Certificate Signing Request.

- b Choose a path and filename, and click **Generate**.

The default file name is `certreq.csr`.

A CSR file is generated in the current working directory.



- 6 Select the CA reply certificate file and click **Import**.

If the CA reply file contains a chain of certificates, the `keytoolgui` utility tries to match the reply's root CA to an existing Trusted Certificate in your cacerts trust store. If this operation fails, the Certificate Details dialog appears for manual verification. Acknowledge the certificate by clicking **OK** and answering **Yes** to the subsequent challenge. Answer **No** if the certificate is not trustworthy for some reason.

After the key pair you generated has been updated to reflect the content of the CA reply, the key store named `keystore.request` contains both the private key and the signed certificate (in the alias `mykey`).

- 7 Choose **Save** from the File menu or the toolbar.

The key store is now ready for use by the ArcSight Manager or ArcSight Web.

- 8 Rename `<ARCSIGHT_HOME>/config/jetty/keystore` to `<ARCSIGHT_HOME>/config/jetty/keystore.old`.

If, for any reason, the new key store does not work properly, you can revert back to the demo key store by replacing `keystore.old` with the new keystore.

For ArcSight Web, rename the file to `webkeystore.old`.

- 9 Copy `<ARCSIGHT_HOME>/config/jetty/keystore.request` to `<ARCSIGHT_HOME>/config/jetty/keystore`.

For ArcSight Web, copy `webkeystore.request` to `webkeystore`.

- 10 If your Manager clients trust the CA that signed your server certificate, go to [Step 12](#).

Otherwise, perform these steps to update the client's cacerts (trust store):



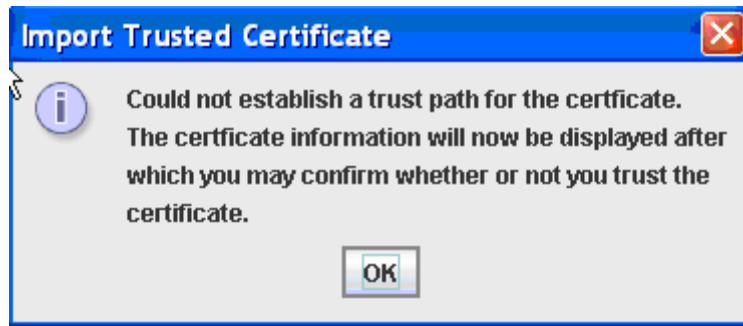
**Note**

You also need to perform these steps on the Manager to update the Manager's cacerts so that Manager clients such as the archive utility can work.

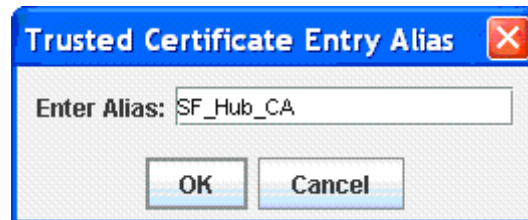
- a Obtain a root certificate from the CA that signed your server certificate and copy it to your client machine.
- b For one client, use the `keytoolgui` utility to import the certificate into the trust store (cacerts):
  - i In `<ARCSIGHT_HOME>/bin`, run this command:
 

```
./arcsight keytoolgui
```
  - ii Click **File->Open Keystore**.
  - iii Select the store named cacerts. Use the password `changeit` to open cacerts.
  - iv Click **Tools->Import Trusted Certificate** and select the certificate you copied in Step 10a of this procedure.

- v You will see the following message. Click **OK**.



- vi Enter an alias for the Trusted Certificate you just imported and click **OK**.



- vii Right-click the alias **ca** in the trust store and choose **Delete** from the menu.
  - viii Save the key store.
- c** Copy the `<ARCSIGHT_HOME>/jre/lib/security/cacerts` file from the client in the previous step to all other clients.
- 11** If your ArcSight Web browser clients trust the CA that signed your ArcSight Web certificate, go to [Step 12](#).
- Otherwise, perform these steps:
- a** Obtain a root certificate from the CA that signed your ArcSight Web certificate.
  - b** Import the certificate into your web browser. See your browser's documentation for details.
- 12** Restart the Manager process.



**Note**

Clients will lose connectivity to the Manager after you restart it. However, you will be able to reconnect the clients after you perform the next step.

- 13** Restart all clients.
- 14** To verify that the new certificate is being used, point a web browser that trusts the CA, which signed the certificate, to ArcSight Web or connect to the Manager using your Console.

## Replacing an Expired Certificate

When a certificate in your truststore/cacerts expires, you need to replace it with a new one. To replace the certificate:

- 1** Delete the expired certificate from the truststore/cacerts.



To delete a certificate from the truststore or cacerts, start the keytoolgui and navigate to the certificate, right-click on the certificate, and select **Delete**.

- 2 Replace the certificate by importing the new certificate into truststore/cacerts as the case may be. Use the keytoolgui to import the new certificate into the truststore or cacerts. See [“Using a Demo Certificate” on page 47](#), [“Using a Self-Signed Certificate” on page 48](#), or [“Using a CA-Signed Certificate” on page 52](#) section (depending on the type of certificate you are importing) for steps on how to import the certificate.

Since the common name (CN) for the new certificate is identical to the CN in the old certificate, you are not permitted to have both the expired as well as the new certificate co-exist in the truststore, cacerts.

## Establishing SSL Client Authentication

By default, clients (SmartConnectors, Consoles, and ArcSight Web) authenticate using user name and password. The clients can optionally use SSL authentication for clients. If SSL client authentication is enabled, you can optionally disable user name and password login, as described in the next section.

When client-side authentication is used, the SSL clients contain a key store and the SSL server contains a trust store.



**Note**

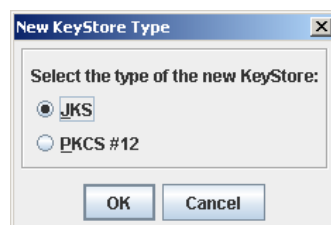
Before you enable client-side authentication, make sure that you log in to the Console and create a new user or modify an existing user such that you set the user's `external_id` to the one specified in the certificate created on the Console. The external id should be set to the users name set as the CN (Common Name) setting when creating the certificate.

## Setting up SSL Client-Side Authentication on ArcSight Console running in Default Mode

If you want to enable client-side authentication for ArcSight Console running in default mode, perform these steps in addition to the ones you perform for setting up server authentication:

- 1 On each Console, generate a key pair. For CA-signed certificate follow the steps in section [“Obtaining a CA-signed certificate” on page 52](#).:
  - a From the Console's `<ARCSIGHT_HOME>/bin` directory start the keytoolgui by running the following command:
 

```
./arcsight keytoolgui
```
  - b Open **File->New Keystore**. This will open the New Keystore Type dialog.
  - c Select **JKS** and click **OK**.



- d Click **Tools->Generate Key Pair** and fill in the fields in the following dialog:



Note

The Common Name (CN) field in the following screen should be the external ID of the user that will be logging in to the Manager that this console will be connecting to.

The 'Generate Certificate' dialog box contains the following fields and buttons:

- Validity (days):
- Common Name (CN):
- Organisation Unit (OU):
- Organisation Name (O):
- Locality Name (L):
- State Name (ST):
- Country (C):
- Email (E):
- Buttons: OK, Cancel

- e Enter an alias for the key pair in the following dialog and click **OK**:

The 'Key Pair Entry Alias' dialog box contains the following fields and buttons:

- Enter Alias:
- Buttons: OK, Cancel



Caution

If you plan to install the Console, Manager, and Web on the same machine, make sure that this alias is unique. Also, make sure not to use the machine name or IP address for the alias. ArcSight Web and Console cannot have identical CNs when installed on the same machine as the Manager.

When you install ArcSight Web, you will be required to set the CN of the ArcSight Web's key pair you generate to the name or IP address of the machine on which you are installing it. Hence, if both Web and Console are on the same machine, and if you use the machine name or IP address for the CN for both the Web and the Console, then ArcSight Web will give you an error when configuring.

- f Enter a password for the keystore and confirm it and click **OK**.

The 'Key Pair Entry Password' dialog box contains the following fields and buttons:

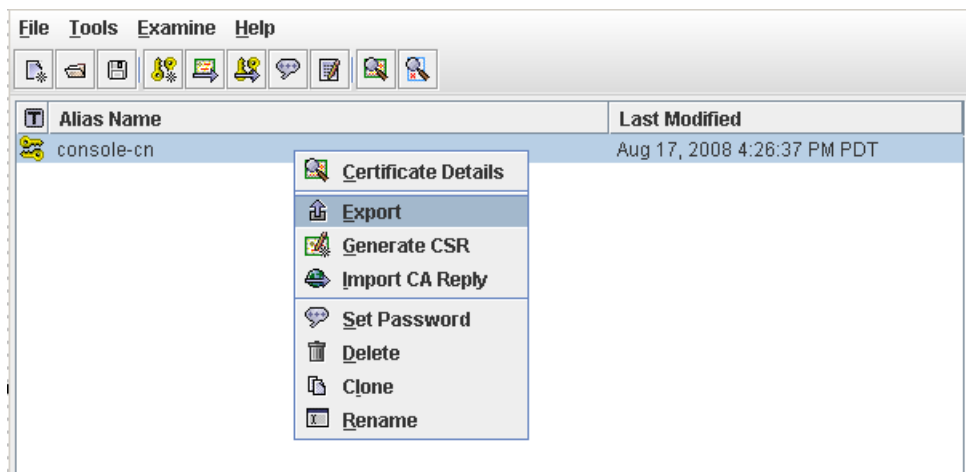
- Enter New Password:
- Confirm New Password:
- Buttons: OK, Cancel

- g You will see the following message.

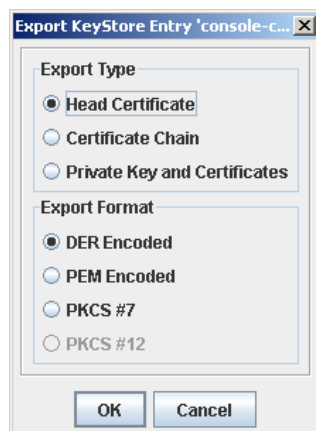


- 2 Export the key pair you just generated.

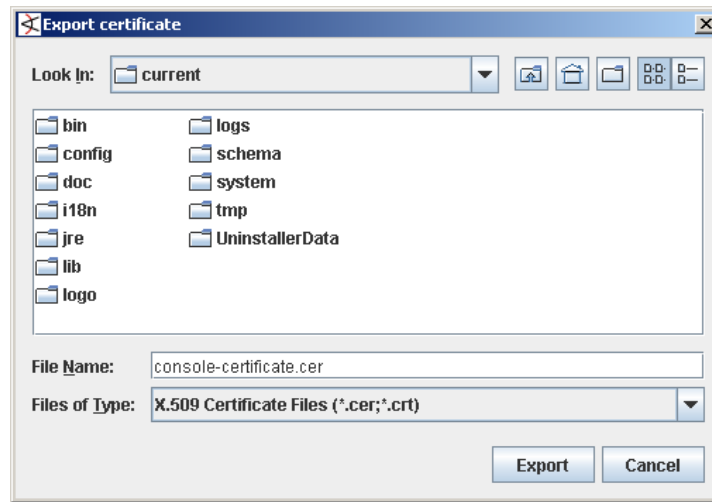
- a In the keytoolgui right-click the key pair you just generated and select **Export**.



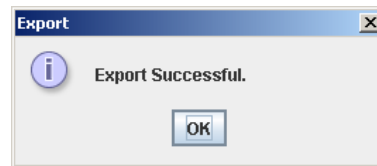
- b Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- c Enter a name for the certificate and click **Export**.



- d You will see the following message:



- e If your Console is on a different machine than the Manager, copy this certificate to the Manager's machine.
- 3 If you are using self-signed certificate skip this step and continue with step 4.

Import the signed certificate response in the keystore of all Consoles.

- ◆ Import the signed certificate response in the Console's keystore, `keystore.client`. Follow the steps in section [“Importing a CA-signed certificate into Manager's truststore” on page 54](#).
- ◆ Use the `changepassword` tool to set an encrypted key store password in the `client.properties` file:  

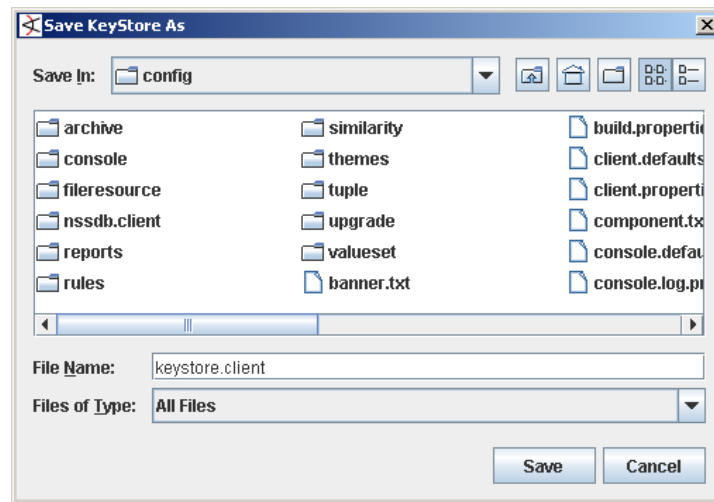
```
arcsight changepassword -f config/client.properties -p ssl.keystore.password
```

- 4 Save the keystore in the Console's `<ARCSIGHT_HOME>/config` directory by clicking on **File->Save KeyStore**.

- a Enter a password for the keystore and confirm it.



- b** Enter `keystore.client` (name for the keystore) in the File Name text box and click **Save**.



- 5** Change the following properties in the Console's `<ARCSIGHT_HOME>/config/client.properties` file and save the file:
- ```
ssl.keystore.password=<set-this-to-password-set-when-you-saved-the-keystore>

ssl.keystore.path=config/keystore.client

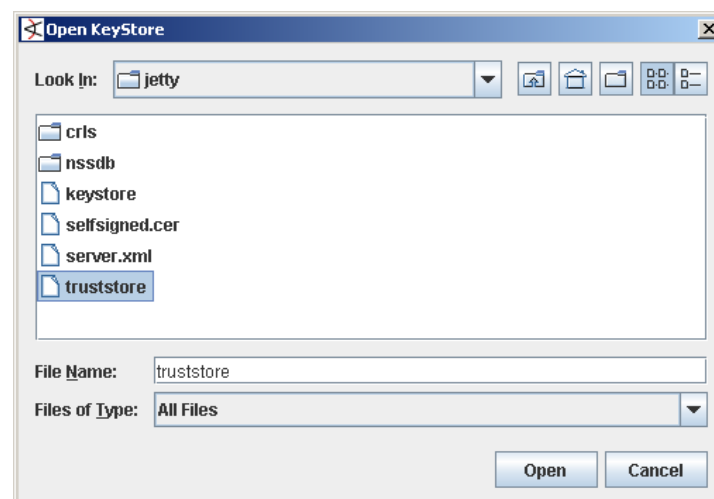
ssl.client.auth=true
```

Make sure that you do not change the keystore name to anything other than `keystore.client`.

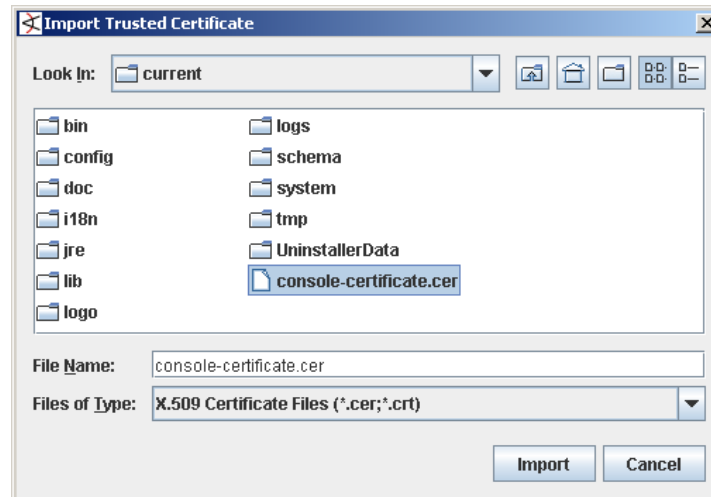
- 6** Import Console's certificate into the Manager's truststore.

If your Manager trusts the CA that signed your Console's certificates, go to the next step. Otherwise perform these steps to update the Manager's truststore.

- a** Start the `keytoolgui` by entering `arcsight keytoolgui` command from the Manager's bin directory.
- b** Click **File->Open KeyStore** and navigate to Manager's `<ARCSIGHT_HOME>/config/jetty/truststore`.



- c Enter "changeit" (without the quotes) when prompted for the password and click **OK**.
- d Click **Tools->Import Trusted Certificate**.
- e Navigate to the Console's certificate that you exported earlier and click **Import**.



- f You will see the following message. Click **OK**.



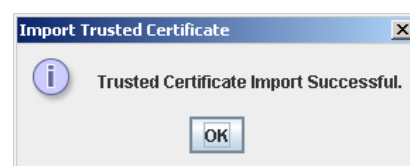
- g Review the certificate details and click **OK**.
- h Click **Yes** in the following dialog.



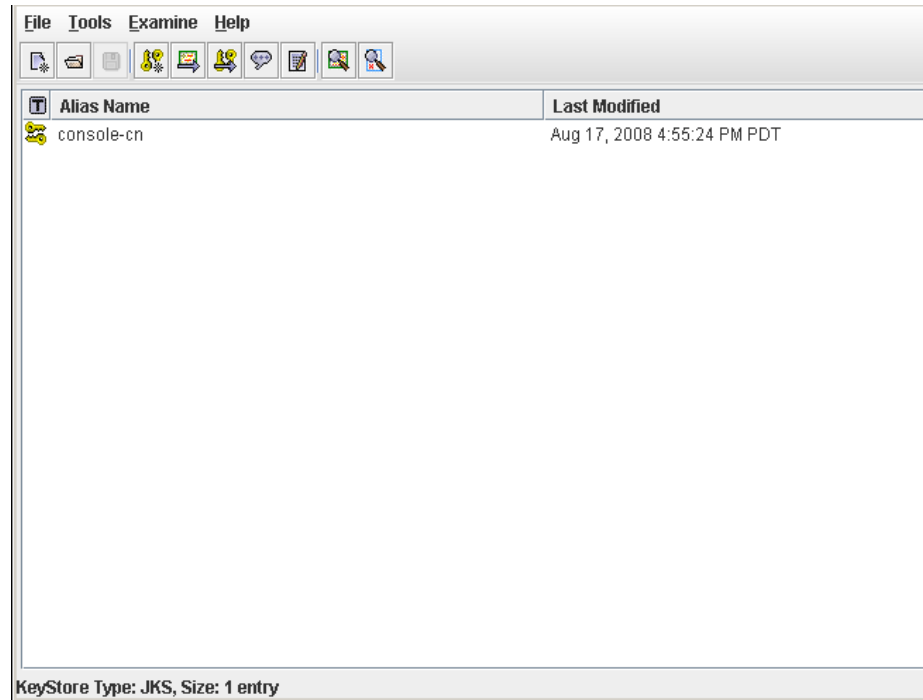
- i Enter an alias for the certificate.



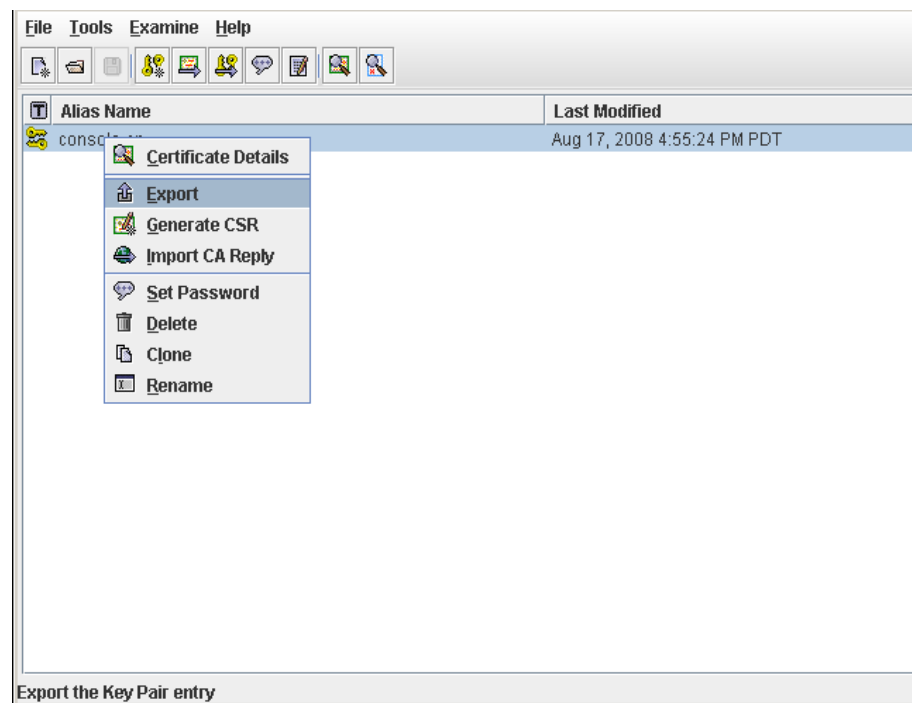
- j You will get the following message if the import was successful.



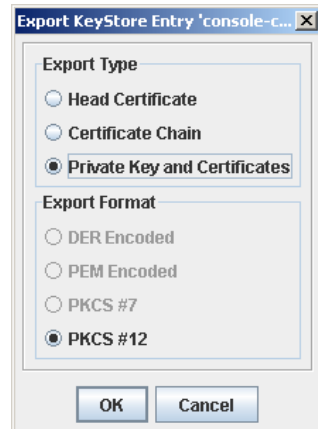
- k** Click **OK** and save the changes to the truststore.
- 7** Export the Console's private key. If you use ArcSight Web, you are required to import the Console's private key into the Web browser you use with ArcSight Web.
  - a** Start the keytoolgui from the Console's `bin` directory.
  - b** Click on **File->Open KeyStore** and navigate to the Console key store you created.



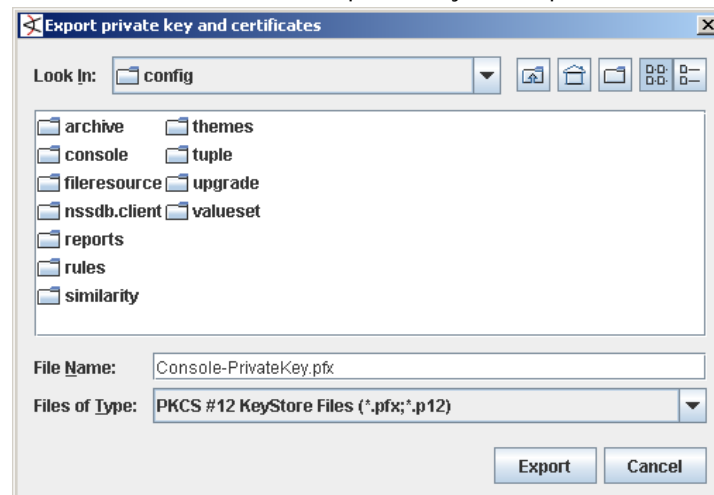
- c** Right-click on the Console's key pair and select Export.



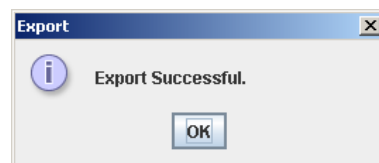
- d Select **Private Key and Certificates** as Export Type and **PKCS#12** as the Export Format if not already selected and click **OK**.



- e Enter the password that you had set for the Console's keystore when prompted and click **OK**.
- f Enter a new password for the keystore and confirm the password and click **OK**.
- g Enter a name for the Console's private key with a .pfx extension and click **Export**.



- h You will receive a message saying Export Successful. Click **OK** and exit the keytoolgui.



- 8 Exit keytoolgui.
- 9 Restart the Manager.
- 10 Restart ArcSight Console.



## Setting up SSL Client Authentication on ArcSight Web

If you want to enable client-side authentication for clients running in default mode, perform these steps in addition to the ones you perform for setting up server authentication:

- 1 Generate a key pair on ArcSight Web. For CA-signed certificate follow the steps in section [“Obtaining a CA-signed certificate” on page 52](#)

- a From the Web's `<ARCSIGHT_HOME>/bin` directory start the keytoolgui by running the following command:

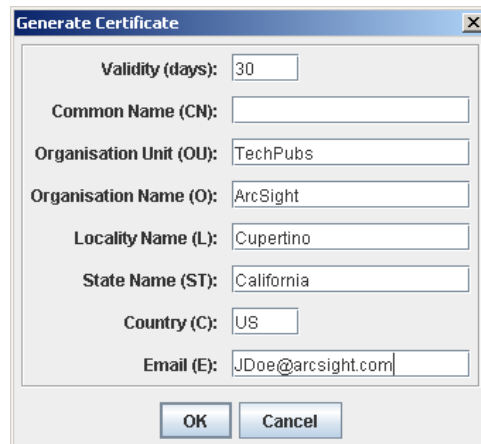
```
./arcsight keytoolgui
```

- b Open **File->New Keystore**. This will open the New Keystore Type dialog.

- c Select **JKS** and click **OK**.



- d Click **Tools->Generate Key Pair** and fill in the fields in the following dialog:

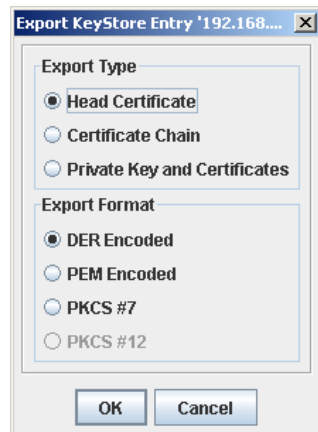


**Note**

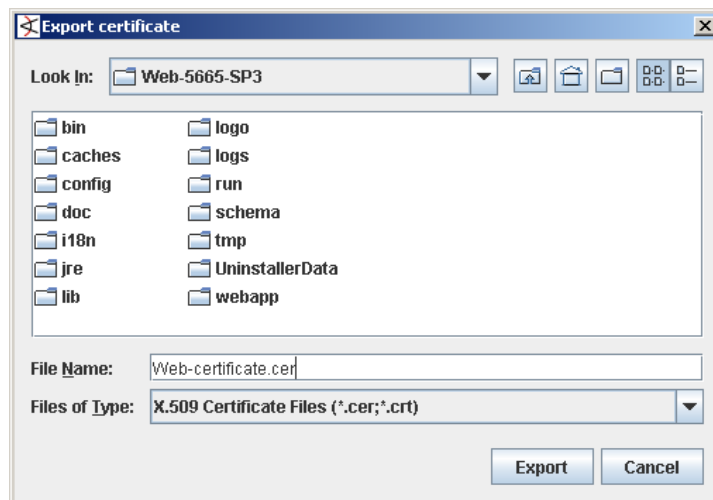
Make sure to use the machine name or IP address on which ArcSight Web is installed for the CN name.

- e Enter an alias for the key pair and click **OK**.
- 2 Export the key pair you just generated.
  - a In the keytoolgui right-click the key pair you just generated and select **Export Key pair**.

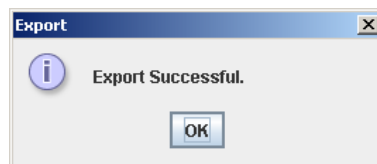
- b** Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



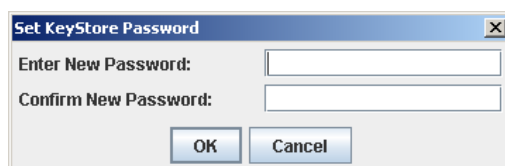
- c** Enter a name for the certificate and click Export.



- d** You will see the following message:



- e** If your ArcSight Web is on a different machine than the Manager, copy this certificate to the Manager's machine.
- 3** Save the keystore in the Web's `<ARCSIGHT_HOME>/config` directory by clicking on **File->Save KeyStore**.
- a** Enter a password for the keystore and confirm it.

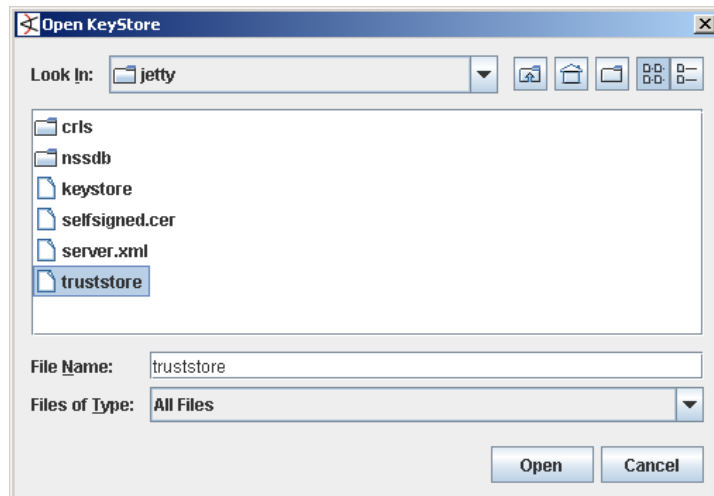


- b Give the keystore a name and click **Save**.
- 4 If you are using self-signed certificate skip this step and continue with step 5.  
Import the signed certificate response in the keystore of ArcSight Web.
  - ◆ Import the signed certificate response in the Web's keystore. Follow the steps in section ["Importing a CA-signed certificate into Manager's truststore" on page 54](#).
  - ◆ Use the `changepassword` tool to set an encrypted key store password in the `client.properties` file:
 

```
arcsight changepassword -f config/client.properties -p
ssl.keystore.password
```
- 5 Add the following properties in the Web's `<ARCSIGHT_HOME>/config/client.properties` file and save the file:
 

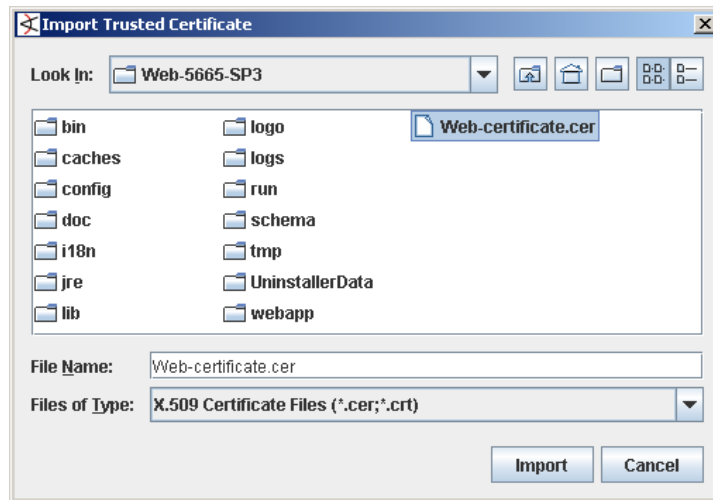
```
ssl.keystore.password=<password-set-when-you-saved-the-keystore>

ssl.keystore.path=config/jetty/webkeystore
```
- 6 Import Web's key pair into the Manager's truststore.  
If your Manager trusts the CA that signed your client's certificates, go to the next step. Otherwise perform these steps to update the Manager's truststore.
  - a Start the keytoolgui by entering `arcsight keytoolgui` command from the Manager's bin directory.
  - b Click **File->Open KeyStore** and navigate to `<ARCSIGHT_HOME>/config/jetty/truststore`.



- c Enter "changeit" (without the quotes) when prompted for the password and click **OK**.
    - d Click **Tools->Import Trusted Certificate**.

- e Navigate to the Web's certificate that you exported earlier and click **Import**.



- f You will see the following message. Click **OK**.



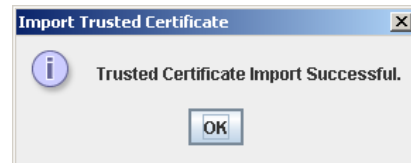
- g Review the certificate details and click **OK**.

- h Click **Yes** in the following dialog.



- i Enter an alias for the certificate.

- j You will get the following message if the import was successful.

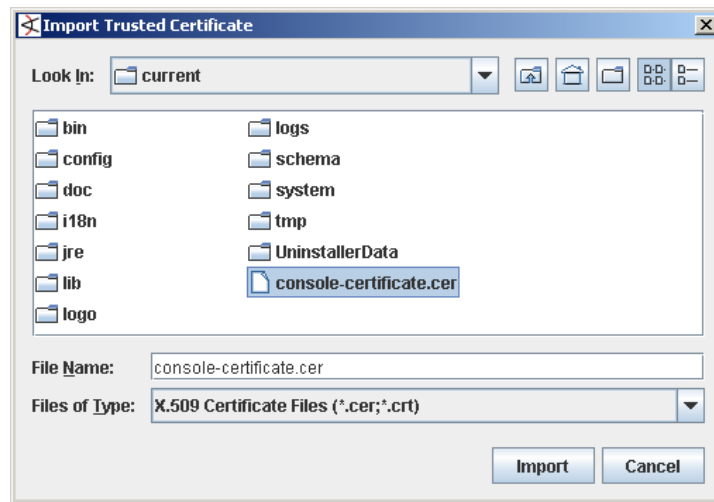


- k Click **OK** and save the changes to the truststore.

**7** Import Console's certificate into webtruststore.

- a Start the keytoolgui from ArcSight Web's `bin` directory.
- b Click **File->Open KeyStore** and navigate to the Web's `<ARCSIGHT_HOME>/config/jetty/webtruststore`.
- c Enter "changeit" (without quotes) when prompted for password.

- d** Click **Tools->Import Trusted Certificate**.



- e** Navigate to the Console's certificate and click **Import**.
- f** Click **OK** in the next message box prompting you that "Could not establish a trust path for the certificate..."
- g** View the certificate details and click **OK**.
- h** Click **Yes** when prompted whether you want to accept the certificate as trusted.
- i** Enter an alias for the console's certificate and click **OK**.
- j** You will see a message saying "Trusted Certificate Import Successful."
- k** Click **OK**.
- l** Save changes to the webtruststore and exit the keytoolgui.
- 8** Import the following into the web browser that you will be using with ArcSight Web:
- ◆ Web's certificate you exported in [Step 2 on page 65](#) above.
  - ◆ Console's private key you created in [Step 7 on page 63](#) in section "Setting up SSL Client-Side Authentication on ArcSight Console running in Default Mode" on [page 57](#).
- See your web browser's documentation for steps to do the above.
- 9** Restart the Manager.
- 10** Restart ArcSight Web.

## Setting up Client-side Authentication on Partition Archiver and SmartConnectors

In order to enable client-side authentication on clients (Partition Archiver and/or SmartConnectors) running in default mode, perform these steps:

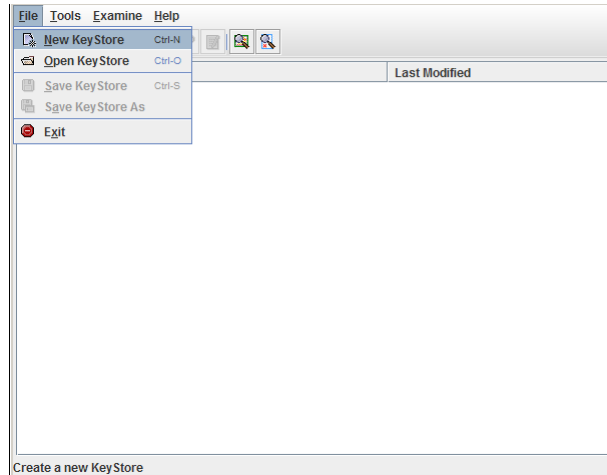
- 1** Create a new client keystore in the ArcSight Database's (for Partition Archiver) or the SmartConnector's `/config` directory.
  - a** Start the keytoolgui from the client's `bin` directory by running the following:  
On SmartConnector:

```
./arcsight agent keytoolgui
```

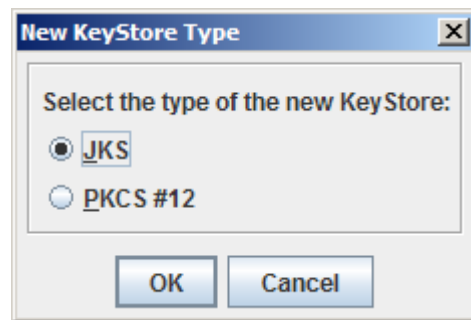
On Partition Archiver:

```
arcsight keytoolgui
```

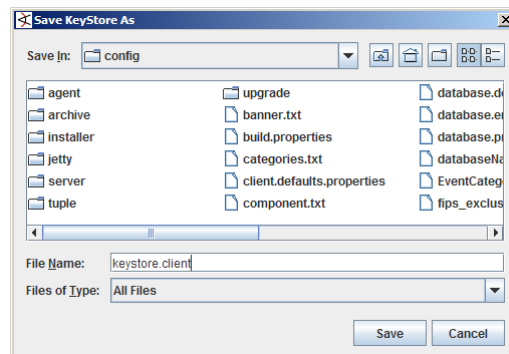
- b** Go to **File->New KeyStore**.



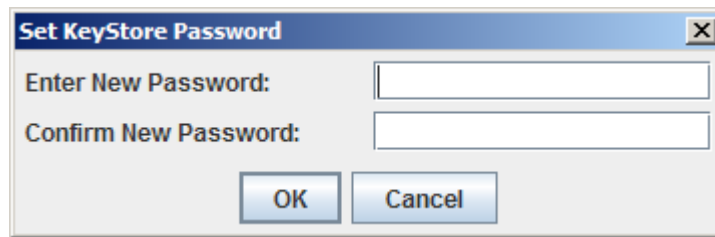
- c** Select **JKS** for type of keystore and click **OK**.



- d** Save the keystore by clicking **File->Save KeyStore As**, navigate to the `config` directory, enter `keystore.client` in the File Name box and click **Save**.

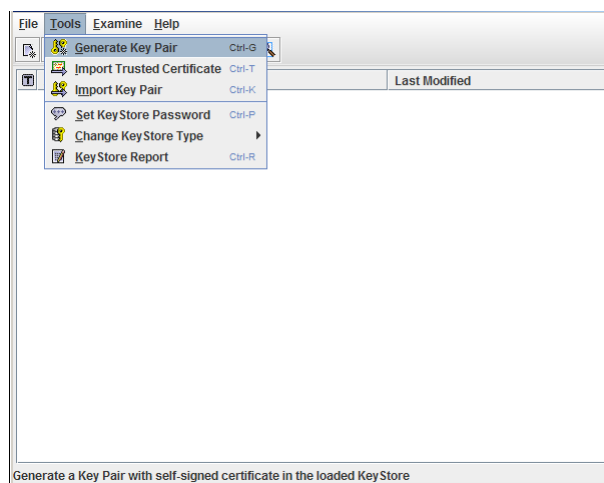


- e Set a password for the keystore and click **OK**.

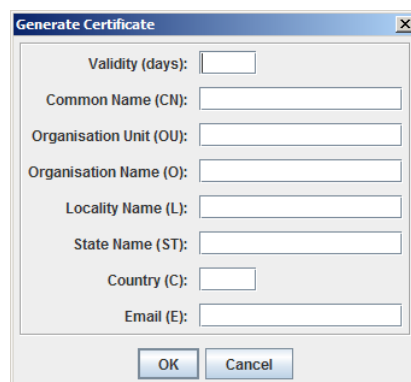


- 2 Create a new keypair in the `config/keystore.client` of the ArcSight Database or SmartConnector. (If you already have a keypair that you would like to use, you can import the existing keypair into the client's `config/keystore.client`. See section "Using Keytoolgui to Import a Key Pair" on page 40 for details.)

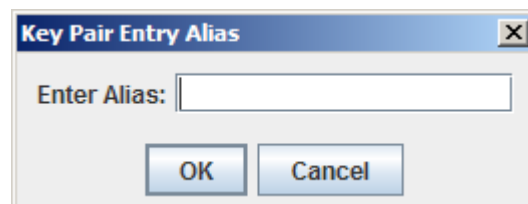
- a In keytoolgui, click **Tools->Generate Key Pair**.



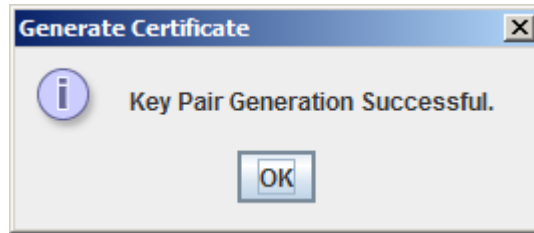
- b In the Generate Certificate dialog enter the details requested and click **OK**.



- c Enter an alias for the key pair and click **OK**.



- d Set a password for the key pair and click **OK**.
- e You will see the following message after the key pair is created. Click **OK**.



You should now see a key pair with the alias you set for it in the keystore.

- 3 Create a client SSL configuration text file in the `config` directory and name it `client.properties`. The contents of `config/client.properties` file should be as follows:

```
auth.null=true

ssl.client.auth=true

cac.login.on=false

ssl.keystore.path=config/arcsightkeystore.client

ssl.keystore.password=<client.keystore_password>
```



Make sure that this password is identical to the password that you set for `/config/keystore.client` when creating it.

- 4 Export the client's (Partition Archiver or Connector) certificate using keytoolgui. See section "Using Keytoolgui to Export a Certificate" on page 40 for details.
- 5 Import the CA's certificate of the client's certificate (in case you are using CA-signed certificate) or the client's certificate itself (in case you are using a self-signed certificate) into the Manager's truststore, `/config/jetty/truststore`. see section "Using Keytoolgui to Import a Certificate" on page 42 for details.
- 6 Restart the Manager.
- 7 Restart the client (Partition Archiver or Connector).

## Migrating from one certificate type to another

When you migrate from one certificate type to another on the Manager, you have to update all Consoles, SmartConnectors, and ArcSight Web installations.

### Migrating from Demo to Self-Signed

To migrate from a demo to self-signed certificate:

- 1 Follow the steps described in "Using a Self-Signed Certificate" on page 48.
- 2 Follow the instructions in "Verifying SSL Certificate Use" on page 73 to ensure that a self-signed certificate is in use.

### Migrating from Demo to CA-Signed

To migrate from a demo to CA-Signed certificate:



- 1 Follow the steps described in [“Using a CA-Signed Certificate” on page 52](#).
- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 73](#) to ensure that CA-signed certificate is in use.

## Migrating from Self-Signed to CA-Signed

To migrate from a self-signed to CA-signed certificate:

- 1 Follow the steps described in [“Using a CA-Signed Certificate” on page 52](#).
- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 73](#) to ensure that a CA-signed certificate is in use.

## Verifying SSL Certificate Use

After the migration, run this command in `<ARCSIGHT_HOME>/bin` on the client to ensure the certificate type you intended is in use:

```
./arcsight tempca -i
```

In the resulting output, a sample of which is available below, do the following:

- 1 Review the value of the line: `Demo CA trusted`.

The value should be “no.”

If the value is “yes,” the demo certificate is still in use. Follow these steps to stop using the demo certificate:

- a In `<ARCSIGHT_HOME>/bin`, enter the following command to make the client stop using the currently in use demo certificate:

```
./arcsight tempca -rc
```

For SmartConnectors, run:

```
./arcsight agent tempca -rc
```

- b Restart the client.

- 2 Verify that the Certificate Authority that signed your certificate is listed in the output.

For a self-signed certificate, the Trusted CA will be the name of the machine on which you created the certificate

## Sample output for verifying SSL certificate use

This is a sample output of the `arcsight tempca -i` command run from a Console's `bin` directory on the Windows platform:

```
ArcSight TempCA starting...
```

```
SSL Client
```

```
Trust Store C:\arcsight\Console\current\jre\lib\security\cacerts
```

```
Type JKS
```

```
Demo CA trusted no
```

```
Trusted CA          DigiCert Assured ID Root CA
[digicertassuredidrootca]

Trusted CA          TC TrustCenter Class 2 CA II
[trustcenterclass2caii] .

.

Demo CA

Key Store  C:\arcsight\Console\current\config\keystore.temppca

Exiting...
```

## Using Certificates to Authenticate Users to ArcSight

Instead of using a user name and password to authenticate a user to ArcSight Manager or ArcSight Web, you can configure these systems to use a digitally-signed user certificate. This section tells you how to do that. You can use Manager's this capability in environments that make use of Public Key Infrastructure (PKI) for user authentication.

The Manager and ArcSight Web accept login calls with empty passwords and use the Subject CN (Common Name) from the user's certificate to identify the user.



Before you enable client-side authentication, make sure that you log in to the Console and create a new user or modify an existing user such that you set the user's `external_id` to the one specified in the certificate created on the Console. The external id should be set to the users name set as the CN (Common Name) setting when creating the certificate.

---

You must enable SSL client authentication as described in the previous section to use digitally-signed user certificates for user authentication.

To configure the Manager or ArcSight Web to use user certificates, do the following:

- 1 On the Console, make sure that External ID field in the User Editor for every user is set to a value that matches the CN in their user certificate.
- 2 Restart the system you are configuring.
- 3 Restart the Consoles.

When you start the Console, the user name and password fields will be grayed out. Simply select the Manager to which you want to connect and click **OK** to log in.

## Using the Certificate Revocation List (CRL)

ArcSight ESM supports the use of CRL to revoke a CA-signed certificate which has been invalidated. The CA that issued the certificates also issues a CRL file which contains a signed list of certificates which it had previously issued that it now considers invalid. ArcSight Manager checks the client certificates against the list of certificates listed in the CRL and denies access to clients whose certificates appear in the CRL.

Before you use the CRL feature, make sure:

- Your certificates are issued/signed by a valid Certificate Authority or an authority with an ability to revoke certificates.

- The CA's root certificate is present in the Manager's `<ARCSIGHT_HOME>/config/jetty/truststore` directory.  
The Manager validates the authenticity of the client certificate using the root certificate of the signing CA.
- You have a current CRL file provided by your CA.  
The CA updates the CRL file periodically as and when additional certificates get invalidated.

To use the CRL feature:

- 1 Make sure you are logged out of the Console.
- 2 Copy the CA-provided CRL file into your Manager's `<ARCSIGHT_HOME>/config/jetty/crls` directory.

After adding the CRL file, it takes approximately a minute for the Manager to get updated.

## Reconfiguring the ArcSight Console after Installation

You can reconfigure ArcSight Console at anytime by typing `arcsight consolesetup` within a command prompt window.

Run the ArcSight Console Configuration Wizard by entering the following command in a command window in the `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight consolesetup
```

To run the ArcSight Console Setup program without the graphical user interface, type:

```
./arcsight consolesetup -i console
```

The ArcSight Console Configuration Wizard appears.

## Reconfiguring ArcSight Manager

To reconfigure ArcSight Manager settings made during installation, run the ArcSight Manager Configuration Wizard by typing the following command in a terminal box or command prompt window:

```
./arcsight managersetup
```

The `arcsight managersetup` command opens the ArcSight Manager Configuration Wizard, but you can also run the ArcSight Manager Setup program silently by typing:

```
./arcsight managersetup -i console
```

The ArcSight Manager Configuration Wizard appears to help you re-configure ArcSight Manager.

To change advanced configuration settings (port numbers, database settings, log location, and so on) after the initial installation, change the `server.properties` file. ArcSight's default settings are listed in the `server.defaults.properties` file. You can override these default settings by adding the applicable lines from `server.defaults.properties` to the `server.properties` file. These files are located in `<ARCSIGHT_HOME>/config`.

## Changing ArcSight Manager Ports

In order for every component of ArcSight to communicate, any ArcSight SmartConnectors and ArcSight Consoles must be aware of what IP address the ArcSight Manager is running on. Also, the ArcSight SmartConnectors and ArcSight Consoles must use the same HTTP or HTTPS port numbers the ArcSight Manager is currently using.

ArcSight Manager uses a single port (by default, 8443) that any firewalls between the ArcSight Manager, ArcSight Console, and any ArcSight SmartConnectors must allow communication through. Port 8443 is the default port used when initially installing ArcSight, however, you can change this default port number using the ArcSight Manager Configuration Wizard. For more information, refer to the *ArcSight ESM Installation and Configuration Guide*.

## Changing ArcSight Web Session Timeouts

The session timeout affects the web browser pages (i.e., Knowledge Base, reports, and so forth) that appear within ArcSight Web. After the session has elapsed, or timed out, you must log back into ArcSight Web to start a new session. You can change the Web default session timeout in this file in the Manager's

`<ARCSIGHT_HOME>/config/jetty/server.xml` file.

The ArcSight Web default session timeout can be changed in this file in ArcSight Web's

`<ARCSIGHT_HOME>/config/jetty/webserver.xml` file.

In the above .xml files you will see the following lines:

```
<session-config>

    <session-timeout>15</session-timeout>

</session-config>
```

The value specified, in this case 15, is the session timeout in minutes. Simply change this number to the session timeout desired and save the file.

## Manager Password Configuration

ArcSight Manager supports a rich set of functionality for managing users passwords. This section describes various password configuration options. Generally, all the settings are made by editing the `server.properties` file. See ["Managing and Changing Properties File Settings" on page 17](#).

## Enforcing Good Password Selection

There are a number of checks that ArcSight Manager performs when a user picks a new password in order to enforce good password selection practices.

### Password Length

The simplest one is a minimum and, optionally, a maximum length of the password. The following keys in `server.properties` affect this:

```
auth.password.length.min=6
auth.password.length.max=20
```

By default, the minimum length for passwords is six characters and the maximum length is 20 characters and can contain numbers and/or letters.

Configuring the above properties to a value of `-1` sets the password length to unlimited characters.

## Restricting Passwords Containing User Name

Another mechanism that enforces good password practices is controlled through the following `server.properties` key:

```
auth.password.userid.allowed=false
```

When this key is set to false (the default), a user cannot include their user name as part of the password.

## Requiring Mix of Characters in Passwords

Good passwords consist not only of letters, but contain numbers and special characters as well. This makes them a lot harder to guess and, for the most part, prevents dictionary attacks.

By default, the minimum length for passwords is six characters and the maximum length is 20 characters and can contain numbers and/or letters.

The following properties control the distribution of characters allowed in new passwords:

```
auth.password.letters.min=-1
```

```
auth.password.letters.max=-1
```

```
auth.password.numbers.min=-1
```

```
auth.password.numbers.max=-1
```

```
auth.password.whitespace.min=0
```

```
auth.password.whitespace.max=0
```

```
auth.password.others.min=-1
```

```
auth.password.others.max=-1
```

The `*.min` settings can be used to enforce that each new password contains a minimum number of characters of the specified type. The `*.max` settings can be used to limit the number of characters of the given type that new passwords can contain. Letters are all letters from A-Z, upper and lowercase, numbers are 0-9; "whitespace" includes spaces, etc.; "others" are all other characters, including special characters such as `#$%&@!`.

Additionally, the following `server.properties` key lets you restrict the number of consecutive same characters allowed.

```
auth.password.maxconsecutive=3
```

For example, the default setting of 3 would allow "adam999", but not "adam9999" as a password.

Furthermore, the following `server.properties` key enables you to specify the length of a substring that is allowed from the old password in the new password.

```
auth.password.maxoldsubstring=-1
```

For example, if the value is set to 3 and the old password is “secret”, neither “secretive” nor “cretin” is allowed as a new password.

## Checking Passwords with Regular Expressions

To accommodate more complex password format requirements, ArcSight Manager can also be set up to check all new passwords against a regular expression. The following `server.properties` keys can be used for this purpose:

```
auth.password.regex.match=
```

```
auth.password.regex.reject=
```

The `auth.password.regex.match` property describes a regular expression that all passwords have to match. If a new password does not match this expression, ArcSight Manager rejects it. The `auth.password.regex.reject` property describes a regular expression that no password may match. If a new password matches this regular expression, it is rejected.



Backslash ( \ ) characters in regular expressions must be duplicated (escaped)—instead of specifying \, type \\.

For more information on creating an expression for this property, see <http://www.regular-expressions.info/>. The following are a few examples of regular expressions and a description of what they mean.

- `auth.password.regex.match= /^[^0-9].*\D$/`

Only passwords that do not start or end with a digit are accepted.

- `auth.password.regex.match= ^(?=[A-Z]{2}[A-Z])(?=[a-z]{2}[a-z])(?=[0-9]{2}[0-9])(?=[^a-zA-Z0-9]{2}[^a-zA-Z0-9]).{10,}$`

Only passwords that contain at least 10 characters with the following breakdown are accepted:

- ◆ At least two upper case letters
- ◆ At least two lower case letters
- ◆ At least two digits
- ◆ At least two special characters (no digits or letters)

- `auth.password.regex.reject= ^(?=[A-Z]{2}[A-Z])(?=[a-z]{2}[a-z])(?=[0-9]{2}[0-9])(?=[^a-zA-Z0-9]{2}[^a-zA-Z0-9]).{12,}$`

The passwords that contain 12 characters with the following breakdown are rejected:

- ◆ At least two upper case letters
- ◆ At least two lower case letters
- ◆ At least two digits
- ◆ At least two special characters (no digits or letters)

## Password Uniqueness

In some environments, it is also desirable that no two users use the same password. To enable a check that ensures this, the following `server.properties` key can be used:

```
auth.password.unique=false
```

If set to true, ArcSight Manager checks all other user's passwords and makes sure nobody else is using the same password.



This feature may not be appropriate for some environments as it allows valid users of the system to guess other user's passwords.

## Setting Password Expiration

ArcSight Manager can be set up to expire passwords after a certain number of days, forcing users to choose new passwords regularly. This option is controlled by the following key in `server.properties`:

```
auth.password.age=60
```

By default, a password expires 60 days from the day it is set.

When this setting is used, however, some problems arise for user accounts that are used for automated log in, such as the user accounts used for Manager Forwarding Connectors. These user accounts can be excluded from password expiration using the following key in `server.properties`:

```
auth.password.age.exclude=username1,username2
```

This value is a comma-separated list of usernames. The passwords of these users never expire.

ArcSight Manager can also keep a history of a user's passwords to make sure that passwords are not reused. The number of last passwords to keep is specified using the following key in `server.properties`:

```
auth.password.different.min=1
```

By default, this key is set to check only the last password (value = 1). You can change this key to keep up to last 20 passwords.

## Restricting the Number of Failed Log Ins

ArcSight Manager tracks the number of failed log in attempts to prevent brute force password guessing attacks. By default, a user's account is disabled after three failed log in attempts. This feature is controlled through the following key in `server.properties`:

```
auth.failed.max=3
```

Change this to the desired number or to `-1` if you do not wish user accounts to be disabled, regardless of the number of failed log in attempts.

Once a user account has been disabled, ArcSight Manager can be configured to automatically re-enable it after a certain period of time. This will reduce the amount of administrative overhead, while at the same time effectively preventing brute force attacks. This mechanism is controlled by the following key in `server.properties`:

```
auth.auto.reenable.time=10
```

This value specifies the time, in minutes, after which user accounts are automatically re-enabled after they were disabled due to an excessive number of incorrect log ins. Set the property key to `-1` to specify that user accounts can only be re-enabled manually.

## Re-Enabling User Accounts

Under normal circumstances, user accounts that have been disabled—for example, as a result of too many consecutive failed log ins—can be re-enabled by any user with sufficient permission. Check the **Enabled** check box for a particular user in the User Inspect/Editor panel in the ArcSight Console.

If there is no user with sufficient privileges remaining enabled—for example, if the only remaining administrator user account is disabled—a command line tool can be run on the system where ArcSight Manager is installed to re-enable user accounts. First, ensure that the ArcSight Manager is running. Then, from the command line, run the following command:

```
./arcsight reenableuser username
```

where username is the name of the user you want to re-enable. After this procedure, the user can log in again, using the unchanged password.

## Properties Related to Domain Field Sets

ESM v5.0 introduces domain field sets, a new construct in the centralized ESM schema that makes it possible to distinguish between events that pertain to different business verticals, such as credit card transactions, online banking, or stock transactions.

The domain field sets feature is separately licensed, and requires some additional configuration on both the Manager and relevant SmartConnectors. See [Chapter 18, Domain Field Sets, on page 489](#) in the *ArcSight ESM User's Guide* for details on this feature.

The following properties related to the Domain Field Sets are configurable in the `server.properties` file on the Manager:

- `domain.event.relevance.percentage`

Using this property, you can set the percentage of additional data fields in an event that must match the pre-defined domain fields in order for the event to be tied to the domain.

For example, if you set this property to `domain.event.relevance.percentage=0.8`, and the additional data in the event has 5 fields, if 4 out of these five fields match the fields defined for a domain, the event is considered to have 80% match. Since you had set this property to .8 (or 80%), the event get tied to that domain and those 4 fields will get persisted. The fifth field that does not match get dropped. Had all five fields matched, all of them would have been persisted. On the other hand, had only 3 fields matched, then the percentage would be less than 80% (minimum percentage that you specified), so the event would not get tied to the domain and all fields (even the 3 that match) would get dropped.

Each event that the connector sends to the Manager can be identified as belonging to a particular pre-configured domain. For events that contains additional data, the fields in the additional data are matched with the fields that are defined for a domain. ESM determines whether the event should be tied to a domain based on the percentage of additional data fields that match the domain fields.

- `domain.ad.keywords.csv`

You can specify which Additional Data fieldname to exclude when additional data in an event is being processed. You can specify the fieldnames to exclude by setting them in this property. Multiple fieldnames can be set as comma separated values. For example,



to exclude integer and date, you would set  
`domain.ad.keywords.csv=Integer,Date.`

## Advanced Configuration Options for Asset Auto-Creation

Assets are automatically created for all components and, if applicable, for assets arriving from scan reports sent by vulnerability scanners via scanner SmartConnectors. This is done by the asset auto-creation feature.

If the profile of events in your network causes asset auto creation feature to create assets in your network model inefficiently, you can modify the asset auto creation default settings in the user configuration file, `server.properties`.

The `server.properties` file is located at  
`$ARCSIGHT_HOME/config/server.properties`.

For more about working with properties files, see the topic “Managing and Changing Properties File Settings”

## Asset Auto-Creation from Scanners in Dynamic Zones

The following properties relate to how assets are created from a vulnerability scan report for dynamic zones.

### Create Asset if either IP Address or Host Name

By default, an asset is not created in a dynamic zone if there is no host name present. The property set by default is:

`scanner-event.dynamiczone.asset.nonidentifiable.create=false`

You can configure ESM to create the asset as long as it has either an IP address or a host name. In `server.properties`, change `scanner-event.dynamiczone.asset.nonidentifiable.create` from `false` to `true`. ESM discards conflicts between an IP address and host name (similar IP address, but different host name and/or MAC address).



**Caution**

**Creating an asset if no host name is present can result in an inaccurate asset model.**

Setting `scanner-event.dynamiczone.asset.nonidentifiable.create` to `true` means that assets are created if the asset has either an IP address or a host name.

This could lead to disabled assets or duplicated assets being created. Change this configuration only if you are using a dynamic zone to host ostensibly static assets, such as long-lived DHCP addresses.

When this property is set to **true**, the following takes place:

Example	Action taken if no conflicts	Action taken if previous asset with similar information
IP=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=myhost mac=null	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=null mac=null	Asset created	Asset created, previous asset is deleted.
ip=null hostname=myhost mac=null	Asset created	Asset created, previous asset is deleted.
ip=null hostname=null mac=0123456789AB	Asset not created. Either host name or IP address is required.	Asset not created. Either host name or IP address is required.
ip=null hostname=myhost mac=0123456789AB	Asset not created. Either host name or IP address is required.	Asset not created. Either host name or IP address is required.

## Preserve Previous Assets

This setting applies when ESM creates assets from a vulnerability scan report for dynamic zones. By default, if a previous asset with similar information already exists in the asset model, ESM will create a new asset and delete the old one.

If you want to preserve the previous asset rather than delete it when a scan finds a new asset with similar information, you can configure ESM to rename the previous asset. In `server.properties`, change `scanner-event.dynamiczone.asset.ipconflict.preserve` from **false** to **true**.



**Caution**

### Preserving previous assets results in a larger asset model.

Setting `event.dynamiczone.asset.ipconflict.preserve` to true means that assets are continually added to the asset model and not removed. Use this option only if you know you must preserve all assets added to the asset model.

When ESM is configured with `scanner-event.dynamiczone.asset.nonidentifiable.create=false` and `scanner-`

`event.dynamiczone.asset.ipconflict.preserve=true`, it takes the following actions:

Example	Action taken if previous asset with similar information and preserve = true
IP=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=myhost mac=null	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=null mac=null	No action taken. Either host name or MAC address is required.
ip=null hostname=myhost mac=null	Asset created, previous asset is renamed.
ip=null hostname=null mac=0123456789AB	Asset created, previous asset is renamed.
ip=null hostname='myhost' mac=0123456789AB	Asset created, previous asset is renamed.

## Changing the Default Naming Scheme

By default, ESM names assets that come from scanners using the naming scheme outlined in the topic [“Asset Names”](#) in the *ArcSight ESM User's Guide*.

	Static Zone	Dynamic Zone
<b>Property:</b>	scanner-event.auto-create.asset.name.template	scanner-event.auto-create.dynamiczone.asset.name.template
<b>Value:</b>	\$destinationAddress - \$!destinationHostName	\$destinationHostName
<b>Example:</b>	1.1.1.1 - myhost	myhost

You can reconfigure this default naming scheme, for example, if you want to show the host name first, or use an underscore to separate the elements.

For example, you want the asset name for an asset in a static zone to appear this way in the ESM UI:

```
myhost_1.1.1.1
```

In this case, change the default

```
$destinationAddress - ${!destinationHostName}
```

to

```
${!destinationHostName}_$destinationAddress
```

## Compression and Turbo Modes

### Enabling Compression for ArcSight SmartConnector Events

ArcSight SmartConnectors can send event information to the ArcSight Manager in a compressed format using HTTP compression. The compression technique used is standard GZip, providing compression ratio of 1:10 or higher, depending on the input data (in this case, the events the ArcSight SmartConnector is sending). Using compression lowers the overall network bandwidth used by ArcSight SmartConnectors dramatically, without impacting their overall performance.

By default, all ArcSight SmartConnectors have compression enabled. To turn it off, add the following line to the `<ARCSIGHT_HOME>/user/agent/agent.properties` file:

```
compression.enabled = false
```

ArcSight SmartConnectors will determine whether the ArcSight Manager they are sending events to supports compression (ArcSight Manager version 2.2 or later).

### Understanding ArcSight Turbo Modes

If your configuration, reporting, and analytic usage permits, you can accelerate the transfer of sensor information through SmartConnectors by choosing one of the "turbo" 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).

ArcSight SmartConnectors can be configured to send more or less event data, on a per-SmartConnector basis, and the ArcSight Manager can be set to read and maintain more or less event data, independent of the SmartConnector setting. Some events require more data than others. For example, operating system syslogs often capture a considerable amount of environmental data that may or may not be relevant to a particular security event. Firewalls, on the other hand, typically report only basic information.

ArcSight defines the following Turbo Modes:

Turbo Modes		
1	Fastest	Recommended for firewalls
2	Faster	Manager default

When Turbo Mode is not specified (mode 3, Complete), all event data arriving at the SmartConnector, including additional data, is maintained. (Versions of ArcSight prior to 3.0 ran in Turbo Mode 3.) Turbo Mode 2, Faster, eliminates the additional custom or vendor-specific data, which is not required in many situations. Turbo Mode 1, Fastest, eliminates

all but a core set of event attributes, in order to achieve the best throughput. Because the event data is smaller, it requires less storage space and provides the best performance. It is ideal for simpler devices such as firewalls.

The ArcSight Manager processes event data using its own Turbo Mode setting. If SmartConnectors report more event data than the Manager needs, the Manager ignores the extra fields. On the other hand, if the Manager is set to a higher Turbo Mode than a SmartConnector, the Manager will maintain fields that are not filled by event data. Both situations are normal in real-world scenarios, because the Manager configuration reflects the requirements of a diverse set of SmartConnectors.

Event data transfer modes are numbered (1 for Fastest, 2 for Faster, 3 for Complete), and possible Manager-SmartConnector configurations are therefore:

1-1 Manager and SmartConnector in Fastest mode

1-2 SmartConnector sending more sensor data than Manager needs

1-3 SmartConnector sending more sensor data than Manager needs

2-1 SmartConnector not sending all data that Manager is storing\*

2-2 Manager and SmartConnector in Faster mode

2-3 Default: Manager does not process additional data sent by SmartConnector

3-1 Manager maintains Complete data, SmartConnector sends minimum\*

3-2 Manager maintains additional data, but SmartConnector does not send it

3-3 Manager and SmartConnector in Complete mode

\*When the SmartConnector sends minimal data (Turbo Mode 1), the Manager can infer some additional data, creating a 2-1.5 or a 3-1.5 situation.

## Configuring the ArcSight Database Monitor

The Database Monitor is an ArcSight Manager component that monitors the ArcSight Database for critical conditions. The Database Monitor performs the following check tasks to ensure that the ArcSight Database can always be used by the ArcSight Manager:

**Free space in Oracle tablespaces:** This check will send an e-mail message if the free space in any of the Oracle tablespaces falls below a specified threshold.

**Database failure:** This check will send an e-mail message if the connection to the database is lost or if the ArcSight Manager detects a fatal, unrecoverable situation in the database, such as lack of disk space.

If a critical condition occurs, the ArcSight Manager will stop accepting incoming events from ArcSight SmartConnectors and, in some cases, will also stop Console sessions. A message is printed to `server.std.log` and `server.log` and sent to a list of administrators via e-mail. The message will contain a URL that can be used to reactivate ArcSight Manager after the problem has been addressed. In many cases, however, the ArcSight Manager can detect that the problem has been resolved and will resume normal operation automatically.

For more information about database checks performed to monitor configuration and runtime attributes of your database, see [Appendix C, Monitoring Database Attributes, on page 169](#).

## Configuring Database Monitor e-mail message recipients

Use the ArcSight Manager Configuration Wizard to configure Database Monitor e-mail message recipients. Run the ArcSight Manager Configuration Wizard by typing `arcsight managersetup` in a command prompt window or terminal box. The ArcSight Notifier is not used for Database Monitor notifications since the ArcSight Manager could already be in such a fatal state that the Notifier may not be able to function properly.

## Configuring the check for free space in Oracle tablespaces

You can set the threshold for checking free space in a tablespace. An e-mail message is sent if the free space in a tablespace falls below the threshold specified. The threshold is specified as a percentage. In `<ARCSIGHT_HOME>\config\server.properties`, set the threshold:

```
databaseinfo.oracle.freespace.percentage.threshold=5
```

You can also explicitly exclude certain tablespaces from the check in `server.properties`. By default, the system tablespace is excluded:

```
databaseinfo.oracle.freespace.exclude tablespaces=SYSTEM
```

## Sending Events as SNMP Traps

ArcSight can send a sub-stream of all incoming events (that includes rule-generated events) via SNMP to a specified target. A filter is used to configure which events will be sent. ArcSight's correlation capabilities can be used to synthesize network management events that can then be routed to your enterprise network management console.

## Configuration of the SNMP trap sender

The SNMP trap sender is configured using the ArcSight Manager configuration file. The `<ARCSIGHT_HOME>/config/server.default.properties` file includes a template for the required configuration values. Copy those lines into your `<ARCSIGHT_HOME>/config/server.properties` file and make the changes there. After making changes to this file, you need to restart the ArcSight Manager.



Setting the Manager to send SNMP v3 traps is not FIPS compliant. This is because SNMP v3 itself uses MD5 algorithm. However, SNMPv1 and v2 are compliant.

---

properties: The following provides a description of specific SNMP configuration parameters:

```
snmp.trapsender.enabled=true
```

Set this property to true in order to enable the SNMP trap sender.

```
snmp.trapsender.uri=
```

```
/All Filters/Arcsight System/SNMP Forwarding/SNMP Trap Sender
```

The filter (specified by URI, all on one line) is used to decide whether or not an event is forwarded. There is no need to change the URI to another filter, as the "SNMP Trap Sender" filter can be changed through the ArcSight Console. Changes to the filter specified will immediately affect the SNMP trap sender. By default, the "SNMP Trap Sender" filter

logic is Matches Filter (Correlated Events)—that is, only rules-generated events will be forwarded.

```
snmp.destination.host=
snmp.destination.port=162
```

The host name and the port of the SNMP listener that wants to receive the traps.

```
snmp.read.community=public
snmp.write.community=public
```

The SNMP community strings needed for the traps to make it through to the receiver. The read community is reserved for future use, however, the write community must match the community of the receiving host. This will depend on your deployment environment and your receiving device. Please consult your receiving device's documentation to find out which community string should be used.

```
snmp.version=1
snmp.fields=\
event.eventId,\
event.name,\
event.eventCategory,\
event.eventType,\
event.baseEventCount,\
event.arcsightCategory,\
event.arcsightSeverity,\
event.protocol,\
event.sourceAddress,\
event.targetAddress
```

These event attributes should be included in the trap. The syntax follows the SmartConnector SDK as described in the *FlexConnector Developer's Guide*. All the ArcSight fields can be sent. The identifiers are case sensitive, do not contain spaces and must be capitalized except for the first character. For example:

ArcSight Field	SDK/SNMP trap sender identifier
Event Name	eventName
Device Severity	deviceSeverity
Service	service

The SNMP field types will be converted as:

ArcSight	SNMP
STRING	OCTET STRING

INTEGER	INTEGER32
Address	IP ADDRESS
LONG	OCTET STRING
BYTE	INTEGER

Additional data values are accessible by name, for example:

```
snmp.fields=event.eventName,additionaldata.myvalue
```

This will send the Event Name field and the value of `myvalue` in the additional data list part of the SNMP trap. Only the String data type is supported for additional data, therefore all additional data values will be sent as `OCTET STRING`.

## Asset Aging

ESM v5.0 introduces two ways in which the age of a scanned asset is taken into consideration. The age of an asset is defined as the number of days since it was last modified. So, for example, if an asset was last modified 29 hours ago, the age of the asset will be taken as 1 day and the remaining time (5 hours, in our example) will be ignored in the calculation of the asset's age.

### Excluding Assets From Aging

To exclude certain assets from aging, you can add those assets to a group and then set the property `asset.aging.excluded.groups.uris` in the `server.properties` file to the URI(s) of those groups.

For example, to add the groups MyAssets and DontTouchThis (both under All Assets) add the following to the `server.properties` file:

```
#Exclude MyAssets and DontTouchThis from aging
asseet.aging.excluded.groups.uris=/All Assets/MyAssets,/All
Assets/DontTouchThis
```



**Note**

When setting the `asset.aging.excluded.groups.uris` property keep in mind that the assets in this group will not be disabled, deleted or amortized.

---

### Task to Disable Assets of a Certain Age

By default, asset aging is disabled. There is a new scheduled task that will disable any scanned asset that has reached the specified age. By default, once the assets aging feature is turned on this task will run every day half an hour after midnight (00:30:00). Add the following in the `server.properties` file to define asset aging:

```
#-----
# Asset aging
#-----
# Defines how many days can pass before a scanned asset is defined
as old
# after this time the asset will be disabled
# Default value: disabled
asset.aging.daysbeforedisable = -1
```



## To Delete an Asset

To delete the asset instead of disabling it, you have to set the property `asset.aging.task.operation` to `delete` in `server.properties` file:

```
# Delete assets when they age

asset.aging.task.operation = delete
```

## Amortize Model confidence with scanned asset age

The `IsScannedForOpenPorts` and `IsScannedForVulnerabilities` subelements in the `ModelConfidence` element will be factored by the age of an asset. they will be extended to include an optional attribute, `AmortizeScan`. If `AmortizeScan` is not defined (or defined with value -1), the assets will not be amortized. A "new" asset will get the full value while and "old" asset will get no points. You can edit the `AmortizeScan` value (number of days) in the Manager's `/config/server/ThreatLevelFormula.xml` file:

```
<ModelConfidence>
  <Sum MaxValue="10" Weight="10">
    <!-- If target Asset is unknown, clamp modelConfidence to 0 -->
    ->
    <HasValue FIELD="targetAssetId" Value="-10" Negated="Yes" />
    <HasValue FIELD="targetAssetId" Value="4" Negated="NO" />
    <!-- Give 4 points each for whether the target asset has been
         scanned for open ports and vulnerabilities -->
    <!-- This values can be amortized by the age of the asset -->
    <!-- that means that the value will reduce constantly over
         time as the asset age -->
    <!-- ie if you set the value to be 120 on the day the assets
         are created they receive the four points, by day 60
         they'll receive 2 points and by day 120 they'll receive 0
         points -->
    <IsScannedForOpenPorts Value="4" Negated="NO"
      AmortizeScan="-1" />
    <IsScannedForVulnerabilities Value="4" Negated="NO"
      AmortizeScan="-1" />
  </Sum>
</ModelConfidence>
```

For this example, the value will be modified as follows:

Asset Age (in days)	AmortizeScan Value
0	4
60	2
120	0
240	0



## Chapter 3

# Database Administration

---

This chapter describes the different tasks that you can perform in order to effectively manage and maintain the ArcSight Database. The topics covered in this chapter include:

[“Changing Oracle Initialization Parameters” on page 91](#)  
[“Monitoring Available Free Space in Tablespace” on page 92](#)  
[“Setting Up Database Threshold Notification” on page 92](#)  
[“Resetting the Oracle Password” on page 92](#)  
[“Oracle Cold Backup” on page 93](#)  
[“Oracle Hot Backup” on page 93](#)  
[“Exporting Data” on page 94](#)  
[“Recovering ArcSight Databases” on page 94](#)  
[“Backing up ArcSight Databases” on page 93](#)  
[“Partition logs” on page 95](#)



To enhance database security and lessen your risk and vulnerability, if you did not use the ArcSight DB Installer to create and configure the ArcSight Database, it is highly recommended that you change the default passwords for the SYS and SYSTEM Oracle user accounts and lock the three accounts DBSNMP, TRACESVR, and OUTLN. In addition, you should delete the following automatically-created Oracle user accounts: ADAMS, BLAKE, CLARK, JONES, and SCOTT. These accounts may have been generated by the Oracle installer.

## Changing Oracle Initialization Parameters

Almost all database parameters can be changed after an instance is created. Some of these parameters are dynamic, whereas many others are static. You can change a dynamic parameter while the instance is running. However, to change a static parameter, you have to change its setting in the initialization parameter file and restart the database to have the modified parameter setting take effect.

Changing these parameters is recommended only for experienced database administrators.

An instance created using an ArcSight template uses a binary version of the initialization parameter file when the database starts up. The binary version (also known as [SPFILE](#)) is, by default, on UNIX:

```
$ORACLE_HOME/dbs/spfile$ORACLE_SID.ora
```

and, on Windows:

```
%ORACLE_HOME%\database\SPFILE%ORACLE_SID%.ORA
```

The ArcSight Installer also generates a text version of the initialization parameter file (also known as `PFILE`), which is, by default, on UNIX:

```
$ORACLE_HOME/admin/$ORACLE_SID/pfile/ini.ora
```

and, on Windows:

```
%ORACLE_HOME%\..\admin\pfile\%ORACLE_SID%.ora
```

When making changes to dynamic parameters, the binary initiation parameter file will be updated automatically. However, Oracle does not synchronize the text version with the binary version automatically. You will have to log in as SYS (use the command, `arcdbutil sql` and type in `/ as sysdba` when prompted for the user name) and run the following command to update the text version:

```
CREATE PFILE='InitParamFilePath' FROM SPFILE
```

Where `InitParamFilePath` is the text version. After making changes to static parameters by editing the text version, you will have to re-start the database. You log in as SYS (use the command, `arcdbutil sql` and type in `/ as sysdba` when prompted for the user name) and run the following command to update the binary version:

```
STARTUP PFILE='InitParamFilePath';
```

If you have the full Oracle license, you can run the `sql / as sysdba` command directly instead of using `arcdbutil`.

Without following these procedures, changes to either version will be lost when the database is re-started.

## Monitoring Available Free Space in Tablespaces

Write scripts to alert when the file systems reach a threshold—say 85%. You can use standard `df -k` command on Unix systems.

## Setting Up Database Threshold Notification

The ArcSight Manager can be configured to automatically notify the administrator when an ArcSight tablespace is nearly full. The default threshold setting is in the file `config\server.defaults.properties` (under `<ARCSIGHT_HOME>` on the Manager host):

```
databaseinfo.freespace.warning.threshold=5
```

This example reflects the default setting, which sends an alert when the amount of free space in any of the ArcSight tablespaces for data or indexes falls to 5% or below.

To override the default threshold, copy this line from the read-only file `server.defaults.properties` to `server.properties` and change the threshold value.

## Resetting the Oracle Password

Depending upon your Oracle settings, you may need to reset your password from time to time. Oracle can be set to expire passwords, which will lock out the ArcSight Manager. To

reset or renew the password for the ArcSight Database user (`arcsight` by default), log in to Oracle with `/ as sysdba` and run the following command:

```
ALTER USER arcsight IDENTIFIED BY ArcSightPassword ACCOUNT UNLOCK
```

Oracle database passwords must start with a letter followed by letters, digits, `'_'`, `'#'`, or `'$'`.

If you change the password for the ArcSight Database user, you will have to reconfigure the ArcSight Manager and Partition Archiver to use the new password.

To reconfigure ArcSight Manager password, run the ArcSight Manager Configuration Wizard by typing the following command in a command window on the Manager host in

```
<ARCSIGHT_HOME>\bin:
```

```
arcsight managersetup
```

If you change the password for the ArcSight Database user, run the command `arcsight database pc` to update the password so that Partition Archiver can continue to log in.

## Backing up ArcSight Databases

Database backups are needed as insurance in case of database failure. There are two types of Oracle database backup methods, cold backup and hot backup.

### Oracle Cold Backup

Oracle Cold Backup means bringing down the Oracle database and backing up all the files comprising the Oracle database. Until all database files are backed up/copied, the Oracle database should remain closed. The advantage of a cold image backup is that it is a clean consistent backup which when restored starts up Oracle to the status it was just before going down. The other major advantage is, since it brings down Oracle, it initializes the shared pool, data buffer cache and other memory structures.

Every week a cold Backup should be done by bringing down Oracle. This can be done at the primary site or the remote site. If done on the primary site then irrespective of the database size, the database has to be down for a maximum of 10 minutes before it is started up if the Veritas database edition for Oracle is used.

Veritas's Quick IO provides this functionality by taking a cold backup of the Oracle database and mounting a read-only file system (Viz., `/snap`) which has only the changes to the original database files. So even if the database is very large, it needs to be down only for a short time before it is brought up.

### Oracle Hot Backup

Oracle Hot Backup is also an image backup of Oracle database files. But it only includes Oracle datafiles as part of its backup. This kind of backup is taken when the database is up and running. The database has to be operating in archivelog mode before hot backup can be done. This backup when restored needs a database recovery applied to it from the online logs and archive logs after the database is mounted. Oracle tracks the changes applied during the backup process by generating a lot of redo log files. An Oracle hot backup should be done every day on the primary or target system.

## Exporting Data

Along with these two backup methods, you should perform a full database export to `/dev/null`, not as a substitute backup strategy but to guarantee that no blocks in the database are corrupt. This is suggested since export is the only method to guarantee full table scans of all the objects in the Oracle database.

Database events in `initarcsight.ora` can be set, but they will signal corruption only when such blocks are actually being accessed. Scheduling of these jobs is the job of the Administrator on site. Jobs to be scheduled are:

- Analyze (compute/estimate statistics)
- Backups
- Export
- Any index rebuilds or defragmentation exercise

## Recovering ArcSight Databases

Database recovery from system failures or disk crashes comprises recovering the database to a consistent state by applying the archived logs. Thus, for the database to be able to recover, it has to be operating in `ARCHIVELOG` mode.

The default database behavior is to operate in `NOARCHIVELOG` mode so recovery will not be possible while operating in this mode. In case of a crash, the database has to be either recreated (when the data will be lost) or restored from a cold backup (when the transactions that were applied to the database since the cold backup was done will be lost).

All production databases should operate in `ARCHIVELOG` mode although there is an overhead involved by way of archive log disk writes. Also in `ARCHIVELOG` mode you can take hot backups (when the database is up and running) as opposed to cold backups (when the database is down for the duration of the backup).

The process of recovering the ArcSight Database is no different than recovering any other Oracle database. However, if you require assistance, you can contact your ArcSight support representative for advice and implementation strategies. If you are using your own Oracle software license, contact Oracle.

## Speeding up partition compression

Starting in ArcSight ESM v3.0 SP2 Patch2, the `NOLOGGING` option is disabled by default to allow event data backup and use of DataGuard. As a result, redo log entries are generated for all database operations (including data compression by Partition Compressor), making the compression process appear somewhat slow.

If database backup is not required or DataGuard is not being used, you can speed up the compression process by enabling the `NOLOGGING` option for Partition Compressor.

To enable the `NOLOGGING` option for Partition Compressor, add the following line to the `config\server.properties` file:

```
partition.compress.exchange.table.logging=false
```

## Partition logs

All log entries including the ones for the database partition utilities are written to the `server.log` file on the ArcSight Manager. In addition, the partition entries are duplicated to one of the following log files on the Manager:

`partitionmanager.log`—For Partition Manager logs

`partitioncompressor.log`—For Partition Compressor logs

`partitionarchiver.log`—For Partition Archiver logs

`partitionstatisticsupdater.log`—For Partition Statistics Updater logs

Entries in a duplicate log file are specific to a partition utility and are based on the log filters defined in `<ARCSIGHT_HOME>\config\server.defaults.properties` file for that utility. These duplicate files enable you to easily browse the relevant information about a partition utility. Additionally, these files are attached in e-mail notifications sent from the partition management utilities.

Additional Partition Archiver logs are available on the ArcSight database machine. These logs are more detailed than the ones available on the Manager and are duplicated to `<ARCSIGHT_HOME>\logs\partitionarchiver.log` file on the database machine. Unlike the duplicated Manager log files, this file is not sent in e-mail notifications.

For information about incomplete logs, see the Database section of the Troubleshooting chapter in this guide.





## Chapter 4

# Managing Resources

---

Some administrator tasks necessary to manage ArcSight ESM are performed in the ArcSight Console. The details for performing such tasks are documented in the Online Help and also in the *ArcSight ESM User's Guide*. This chapter points you to the location where these tasks are documented in the *ArcSight ESM User's Guide*.

This chapter in ArcSight <i>ESM</i> User's Guide...	...discusses these topics
Chapter 24, Managing Users and Permissions	<ul style="list-style-type: none"><li>• Managing Users</li><li>• Managing Permissions and Resources</li><li>• Managing Notifications</li></ul>
Chapter 27, Modeling the Network	<ul style="list-style-type: none"><li>• Modeling the Network</li><li>• Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories</li><li>• Managing Customers</li></ul>
Chapter 10, Filtering Events	<ul style="list-style-type: none"><li>• Creating Filters</li><li>• Moving or Copying Filters</li><li>• Deleting Filters</li><li>• Debugging Filters to Match Events</li><li>• Applying Filters</li><li>• Importing and Exporting filters</li><li>• Using Filter Groups</li><li>• Investigating Views</li><li>• Modifying Views</li></ul>

This chapter in ArcSight <i>ESM</i> User's Guide...	...discusses these topics
Chapter 25, Managing Resources	<ul style="list-style-type: none"> <li>• Managing File Resources</li> <li>• Locking and Unlocking Resources</li> <li>• Selecting Resources</li> <li>• Finding Resources</li> <li>• Visualizing Resources</li> <li>• Viewing Resources in Grids</li> <li>• Validating Resources</li> <li>• Extending Audit Event Logging</li> <li>• Saving Copies of Read-Only Resources</li> <li>• Common Resource Attribute Fields</li> <li>• Managing Packages</li> </ul>
Chapter 26, Managing SmartConnectors	<ul style="list-style-type: none"> <li>• Selecting and Setting SmartConnector Parameters</li> <li>• Managing SmartConnector Filter Conditions</li> <li>• Setting Special Severity Levels</li> <li>• Sending Model Mappings to SmartConnectors</li> <li>• Sending Control Commands to SmartConnectors</li> <li>• Managing SmartConnector Groups</li> <li>• Managing SmartConnector Resources</li> <li>• Importing and Exporting SmartConnector Configurations</li> <li>• Upgrading SmartConnectors</li> </ul>
Chapter 28, Managing Partitions	<ul style="list-style-type: none"> <li>• Getting Partition Information</li> <li>• Seeing a Partition Schedule</li> <li>• Archiving Partitions</li> <li>• Reactivating Archived Partitions</li> <li>• Reactivating Zipped or Large Archived Partitions</li> <li>• Deactivating Archived Partitions</li> <li>• Running Scheduled Tasks Right Away</li> <li>• Partition Properties</li> </ul>

## Appendix A

# ArcSight Commands

---

This appendix provides information about ArcSight command scripts and utility programs. This appendix is divided into the following sections:

[“Running an ArcSight Command Script” on page 99](#)

[“Alphabetic List of Commands” on page 100](#)

## Running an ArcSight Command Script

To run an ArcSight command script on a component, open a command window and switch to the `<ARCSIGHT_HOME>/bin` directory. Execute the following command:

```
arcsight command_name [parameters]
```

The following sections describe the supported ArcSight commands.

# Alphabetic List of Commands

## ACLReportGen

<b>Description</b>	A tool for generating a report on ACLs either at the group level or at the user level. By default, the generated report is placed in the <code>/opt/arcsight/manager/ACLReports</code> directory.	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>ACLReportGen &lt;parameters&gt;</code>	
<b>Options</b>	Optional:	
	<code>-config &lt;config&gt;</code>	The primary configuration file (config/server.defaults.properties)
	<code>-locale</code>	The locale to run under
	<code>-m &lt;mode&gt;</code>	Mode in which this tool is run to generate the ACLs report. Supported modes are <ul style="list-style-type: none"> <li>• grouplevel</li> <li>• userlevel</li> </ul> Default value is grouplevel
	<code>-pc &lt;privateConfig&gt;</code>	The override configuration file (config/server.properties)
	<code>-h help</code>	
<b>Examples</b>	To run this tool: <code>arcsight ACLReportGen</code>	

## agent logfu

<b>Description</b>	Graphical SmartConnector log file analyzer	
<b>Applies to</b>	SmartConnectors	
<b>Syntax</b>	<code>agent logfu -a [options]</code>	
<b>Options</b>	<code>-a</code>	SmartConnector log. Required.
		For other options, see <code>logfu</code> command (Manager)
<b>Examples</b>	To run logfu: <code>arcsight agent logfu -a</code>	

## agent tempca

<b>Description</b>	Inspect and manage temporary certificates for a SmartConnector host machine
--------------------	-----------------------------------------------------------------------------

<b>Applies to</b>	SmartConnectors
<b>Syntax</b>	<code>agent tempca</code>
<b>Options</b>	For options, see <code>tempca</code> command (Manager)
<b>Examples</b>	To run: <code>arcsight agent tempca</code>

## agentcommand

<b>Description</b>	Send a command to SmartConnectors
<b>Applies to</b>	SmartConnectors
<b>Syntax</b>	<code>agentcommand -c (restart   status   terminate)</code>
<b>Options</b>	<code>-c</code> Command: <code>restart</code> , <code>status</code> , or <code>terminate</code>
<b>Examples</b>	<p>To retrieve status properties from the SmartConnector:</p> <pre>arcsight agentcommand -c status</pre> <p>To terminate the SmartConnector process:</p> <pre>arcsight agentcommand -c terminate</pre> <p>To re-start the SmartConnector process:</p> <pre>arcsight agentcommand -c restart</pre>

## agents

<b>Description</b>	Run all installed ArcSight SmartConnectors on this host as a standalone application.
<b>Applies to</b>	SmartConnectors
<b>Syntax</b>	<code>agents</code>
<b>Options</b>	None
<b>Examples</b>	<p>To run all SmartConnectors:</p> <pre>arcsight agents</pre>

## agentsetup

<b>Description</b>	Run the SmartConnector Configuration Wizard
<b>Applies to</b>	SmartConnectors
<b>Syntax</b>	<code>agentsetup [-i mode] [-w] [-f file] [-g] [-t type] [-sn name]</code>
<b>Options</b>	<p><code>-a</code> Show connectors for all platforms</p> <p><code>-f file</code> Properties file (required in <code>-i</code> silent mode)</p> <p><code>-g</code> Generate sample properties file for use in <code>-i</code> silent mode</p> <p><code>-h</code> Get help on agentsetup command</p> <p><code>-i mode</code> Mode: silent, console, swing</p>

<code>-R</code>	Re-register an connector
<code>-sn name</code>	Short Name
<code>-t type</code>	SmartConnector Type (overrides short name)
<code>-w</code>	Run in wizard mode

---

**Examples**

To run the SmartConnector Configuration Wizard:

```
arcsight agentsetup
```

---

## agentsvc

<b>Description</b>	Install ArcSight SmartConnector or Partition Archiver as a service.	
<b>Applies to</b>	SmartConnectors and Database	
<b>Syntax</b>	<code>agentsvc -i -u user</code>	
<b>Options</b>	<code>-i</code>	Install the service
	<code>-u</code>	Run service as user user
<b>Examples</b>	To install a SmartConnector or Partition Archiver as a service:	
	<code>arcsight agentsvc</code>	

## agenttempca

<b>Description</b>	See the agent tempca command
<b>Applies to</b>	SmartConnectors

## agentup

<b>Description</b>	Get the current state of a SmartConnector. Returns 0 if the SmartConnector is running and reachable. Returns 1 if not	
<b>Applies to</b>	SmartConnectors	
<b>Syntax</b>	<code>agentup</code>	
<b>Options</b>	None	
<b>Examples</b>	To check that the SmartConnector is up, running, and accessible:	
	<code>arcsight agentup</code>	

## arcdbutil

<b>Description</b>	A utility that enables you to launch database utilities for operations such as <code>import</code> , <code>export</code> , sql interface, <code>backup</code> , <code>restore</code> , and other database commands	
<b>Applies to</b>	Database	
<b>Syntax</b>	<code>arcdbutil database_command command_options</code>	
<b>Options</b>	database_command	Possible commands include: <code>sql</code> , <code>listener</code> , <code>backup</code> , <code>recover</code> , <code>import</code> , <code>export</code> , and other database commands
	command_options	All valid options for the database command you use



**Examples**

---

To identify all disabled rules in your current installation:

```
arcdbutil sql select name from arc_resource where id in  
(select id from arc_rules where active=0);
```

To get an SQL interface:

```
arcdbutil sql  
Enter user-name: / as sysdba
```

---

## arcdt

<b>Description</b>	A utility that enables you run diagnostic utilities such as session wait times, thread dumps, and database alert logs about your ArcSight system, which helps ArcSight Customer Support analyze performance issues on your ArcSight components
<b>Applies to</b>	Manager
<b>Syntax</b>	<pre>arcdt diagnostic_utility utility_options</pre>
<b>Options</b>	<p><code>diagnostic_utility</code> Utilities you can run are:</p> <ul style="list-style-type: none"> <li><code>runsql</code>—Run SQL commands contained in a file that is specified as a parameter of this utility.</li> </ul> <p>Required Parameters:</p> <p><code>-f &lt;sqlfile&gt;</code> The file containing the sql statement to be executed.</p> <p>Optional Parameters:</p> <p><code>-fmt &lt;format&gt;</code> The format the output should be displayed in (where relevant), choices are: html/text (text)</p> <p><code>-o &lt;outputfile&gt;</code> File name to save output to. ()</p> <p><code>-rc &lt;row_count&gt;</code> The number of rows to be shown as a result of a select. (10000)</p> <p><code>-se &lt;sessionEnd&gt;</code> if type is EndTime or mrt, value will be like yyyy-MM-dd-HH-mm-ss-SSS-zzz; if type is EventId, value will be a positive integer indicating the end of eventId. (2011-06-30-01-00-00-000-GMT)</p> <p><code>-sr &lt;start_row&gt;</code> The row number from which you want data to be shown (0)</p> <p><code>-ss &lt;sessionStart&gt;</code> if type is EndTime or mrt, value will be like yyyy-MM-dd-HH-mm-ss-SSS-zzz; if type is EventId, value will be a positive integer indicating the end of eventId. (2011-06-30-00-00-00-000-GMT)</p> <p><code>-t &lt;terminator&gt;</code> The character that separates SQL statements in the input file. (;)</p> <p><code>-type &lt;type&gt;</code> Session type for sql query: EndTime, mrt, or EventId (EndTime)</p> <p>Options:</p> <p><code>-cmt commit</code> - Flag indicating whether all inserts and updates should be committed before exiting.</p> <p><code>-sp spool</code> - Flag specifying whether output should be saved to disk or not.</p> <p><code>db-alertlog</code>—Retrieve the database alert log from the database machine.</p>

- `session-waits`—Retrieve the currently running JDBC (Java Database Connection) sessions and their wait times.

Required Parameters:

`-sp spool` - Flag specifying whether output should be saved to disk or not.

Optional Parameters:

`-c <count>` The number of times we want to query the various session tables. (5)

`-f <frequency>` The time interval (in seconds) between queries to the session tables. (20)

`-fmt <format>` The format the output should be displayed in (where relevant), choices are: html/text (text)

`-o <outputfile>` File name to save output to. ()

- `thread-dumps`—Obtain thread dumps from the Manager. Optional parameters which can be specified

`-c <count>` The number of thread dumps to request. (3)

`-f <frequency>` The interval in SECONDS between each thread dump request. (10)

`-od <outputdir>` The output directory into which the requested thread dumps have to be placed. ()

`utility_options` To see the options available for each utility, run this command in `<ARCSIGHT_HOME>/bin`:

```
arcdt help diagnostic_utility
```

To find out the number of cases in your database:

- 1 Create a file called `sample.txt` in `<ARCSIGHT_HOME>/temp` on the Manager with this SQL command:

```
select count(*) from arc_resource where
resource_type=7;
```

#### Examples

- 2 Run this command in `<ARCSIGHT_HOME>/bin`:

```
arcdt runsql temp/sample.txt
```

To retrieve the last 20 lines of database alert log from your database machine and save it to a file called `20110720_dblog`, run this command:

```
arcdt db-alertlog -ln 20 -o 20110720_dblog
```

## archive

<b>Description</b>	Import or export resources (users, rules, and so on) to or from one or more XML files.
<b>Applies to</b>	Manager, Console
<b>Syntax</b>	<code>archive -f archivefile [options]</code>

Options	<code>-action action</code>	Possible actions include: <code>diff</code> , <code>export</code> , <code>il8nsync</code> , <code>import</code> , <code>list</code> , <code>merge</code> , and <code>sort</code> . Default: <code>export</code> .
	<code>-all</code>	Export all resources in the system (not including events)
	<code>-base basefile</code>	The basefile when creating a migration archive. The new archive file is specified with <code>-source</code> (the result file is specified with <code>-f</code> )
	<code>-config file</code>	Configuration file to use. Default: <code>config/server.defaults.properties</code>
	<code>-exportaction exportaction</code>	The action attribute to assign to each resource object exported. Export actions are:  <code>insert</code> : Insert the new resource if it doesn't exist.  <code>update</code> : Update a resource if it exists.  <code>remove</code> : Remove a resource if it exists.  Default: <code>insert</code>
	<code>-f archivefile</code>	The input (import) or the output (export) file specification. <b>Note:</b> Filename paths can be absolute or relative. Relative paths are relative to <code>&lt;ARCSIGHT_HOME&gt;</code> , not the current directory. Required
	<code>-format fmt</code>	Format of the archive: <code>preferarchive</code> , <code>force</code> , <code>interactive</code> , <code>overwrite</code> or <code>skip</code> . Default: <code>default</code> .  <code>default</code> : Prompts user to resolve import conflicts.  <code>force</code> : Conflicts are resolved by the new overwriting the old.  <code>overwrite</code> : Merges resources, but does not perform any union of relationships.  <code>preferarchive</code> : Merges resources. For example, if a group is imported, the resulting group will contain all its original members and all of the new members from the import file.  <code>skip</code> : Do not import resources with conflicts.
	<code>-h</code>	Get help for this command
	<code>-i</code>	(Synonym for <code>-action import</code> .)
	<code>-m manager</code>	The ArcSight Manager to communicate with

---

<code>-newids</code>	All archival objects within an archive will be given new IDs. All refs to these archival objects will be changed to the new ID or removed if not found. This option is useful when an archive is created and then all resources in the archive are modified to create new resources but the IDs were retained
<code>-o</code>	Overwrite any existing files
<code>-optimizedimport</code>	Performs pre-processing during import for optimization. Forces the import of values even though they are the same as what is stored in the database. If this flag is not set, each of the values in the archive will be compared with the value in the database to determine whether any changes have been made; if no changes are found, then the import for that object will be skipped
<code>-p password</code>	Password with which to log in to the Manager
<code>-param paramfile</code>	The source file for parameters. Any parameters in the paramfile can be overridden by command line values
<code>-pc configfile</code>	Private configuration file to override <code>-config</code> . Default: <code>config/server.properties</code>
<code>-pkcs11</code>	Use this option when authenticating with a PKCS#11 provider. For example,  <code>arcsight archive -m &lt;hostname&gt; -pkcs11 -f &lt;file path&gt;</code>
<code>-port port</code>	The port to use for Manager communication. Default: 8443
<code>-q</code>	Quiet: do not output progress information while archiving
<code>-source sourcefile</code>	The source file used when <code>-f</code> specifies an output file
<code>-standalone</code>	Operate directly on the Database, not the Manager.  <b>Warning:</b> Do not run archive in <code>-standalone</code> mode when the Manager is running; database corruption could result.
<code>-u username</code>	The user name to log in to the Manager with
<code>-uri includeURIs</code>	The URI(s) to export. No effect during import. All dependent resources are exported, as well—for example, all children of a group.  Separate multiple URIs (such as <code>/All Filters/Geographic/West Coast</code> ) with a space, or repeat the <code>-uri</code> switch

---

<code>-urichildren includes</code>	The parent URI(s) to export. No effect during import. All child resources of the specified resources will be exported. The parent resources are only exported if there is a dependency
<code>-xrefids</code>	Exclude reference IDs. This option determines whether to include reference IDs during export. This is intended only to keep changes to a minimum between exports. Do not use this option without a complete understanding of its implications
<code>-xtype excludeTypes</code>	The type(s) to exclude during export. No effect during import. Exclude types must be valid type names, such as Group, Asset, or ActiveChannel
<code>-xtyperef excludeTypes</code>	Same as the <code>-xtype</code> option, but will also exclude all references of the specified type
<code>-xuri excludeURIs</code>	The URI(s) to exclude during export. No effect during import. Resources for which all possible URIs are explicitly excluded will not be exported. Resources which can still be reached by a URI that is not excluded will still be exported
<code>-xurichildren excludes</code>	The parent URI(s) to exclude during export. No effect during import. Resources for which all possible URIs are explicitly excluded will not be exported. Resources which can still be reached by a URI that is not excluded will still be exported.

---

To import resources from an XML file (on a Unix host):

```
arcsight archive -action import -f  
/user/subdir/resfile.xml
```

To export certain resources (the program displays available resources):

```
arcsight archive -f resfile.xml -u admin -m mgrName -p pwd
```

To export all resources to an XML file in quiet, batch mode:

```
arcsight archive -all -q -f resfile.xml -u admin -m  
mgrName -p password
```

To export a specific resource:

### Examples

```
arcsight archive -uri "/All Filters/Geographic/West Coast"  
-f resfile.xml
```

Manual import (program prompts for password):

```
arcsight archive -i -format preferarchive -f resfile.xml -  
u admin -m mgrName
```

Scheduled or batch importing:

```
arcsight archive -i -q -format preferarchive -f  
resfile.xml -u admin -m mgrName -p password
```

Scheduled or batch exporting:

```
arcsight archive -f resfile.xml -u admin -m mgrName -p  
password -uri "/All Filters/Geographic/East Coast" -uri  
"/All Filters/Geographic/South"
```

---

## archivefilter

<b>Description</b>	Use the command to change the contents of the archive. The archivefilter command takes a source archive xml file as input, applies the filter specified and writes the output to the target file.	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>archivefilter -source sourcefile -f archivefile [options]</code>	
<b>Options</b>	<code>-a action</code>	Action to perform { <code>insert</code> , <code>remove</code> , <code>none</code> } (Default: <code>none</code> )
	<code>-e element_list</code>	Elements to process (Default: <code>'*'</code> which denotes all elements)
	<code>-extid regex</code>	Regular expression to represent all of the external IDs to include. This is the external ID of the archival object. (Default: <code>none</code> )
	<code>-f file</code>	Target file (required). If a file with an identical name already exists in the location where you want to create your target file, the existing file will be overwritten. If you would like to receive a prompt before this file gets overwritten, use the <code>-o</code> option
	<code>-o</code>	Overwrite existing target file without prompting (Default: <code>false</code> )
	<code>-relateduri regex</code>	Regular expression to get all of the URIs found in references to include. This will check all attribute lists that have references and if any of them have a URI that matches any of the expressions, that object will be included
	<code>-source file</code>	Source file (required)
	<code>-uri regex</code>	Regular expression to represent all of the URIs to include. This is the URI of the archival object
	<code>-xe element_list</code>	Elements to exclude
	<code>-xextid regex</code>	Regular expression to represent all of the external IDs to exclude
	<code>-xgroups groups</code>	Groups to exclude
	<code>-xuri regex</code>	Regular expression to represent all of the URIs to exclude
	<code>-h</code>	Help for this command



<b>Examples</b>	To include any resources, for example all Active Channels, whose attributes contain the URI specified by the <code>-relateduri</code> option:
	<pre>arcsight archivefilter -source allchannels.xml -f t0.xml -relateduri "/All Active Channels/ArcSight Administration/"</pre>
	To include any resources whose parent URI matches the URI specified by the <code>-uri</code> option:
	<pre>arcsight archivefilter -source allchannels.xml -f t0.xml -uri "/All Active Channels/ArcSight Administration/.*"</pre>
	To exclude resources whose parent URI matches the URI specified by the <code>-xuri</code> option:
	<pre>arcsight archivefilter -source allchannels.xml -f t0.xml -xuri "/All Active Channels/.*"</pre>
	To include all the resources that contain either URIs specified by the two <code>-relateduri</code> options:
	<pre>arcsight archivefilter -source allchannelsFilter.xml -f t0.xml -relateduri "/All Active Channels/ArcSight Administration/" -relateduri ".*Monitor.*"</pre>

## archivewizard

<b>Description</b>	Archive wizard
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>archivewizard</code>
<b>Options</b>	None
<b>Examples</b>	To run: <pre>arcsight archivewizard</pre>

## bleep

<b>Description</b>	Unsupported stress test tool to supply a Manager with security events from replay files (see <a href="#">replayfilegen</a> ). Replay files containing more than 30,000 events require a lot of memory on the bleep host.
	Do not run bleep on the Manager host. Install the Manager on the bleep host and cancel the configuration wizard when it asks for the Manager's host name.
	Run <code>arcsight tempca -ac</code> on the bleep host if the Manager under test is using a demo certificate.
	Create the file <code>config/bleep.properties</code> using the descriptions in <code>bleep.defaults.properties</code> .
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>bleep [-c file] [-D key=value [key=value...]]</code>

<b>Options</b>	<code>-c file</code>	Alternate configuration file (default: <code>config/bleep.properties</code> )
	<code>-D key=value</code>	Override definition of configuration properties
	<code>-m n</code>	Maximum number of events to send. (Default: -1)
	<code>-n host</code>	Manager host name
	<code>-p password</code>	Manager password
	<code>-t port</code>	Manager port (Default: 8443)
	<code>-u username</code>	Manager user name
	<code>-h</code>	Display command help
<b>Examples</b>	To run:	
	<code>arcsight bleep</code>	

## bleepsetup

<b>Description</b>	Wizard to help create the <code>bleep.properties</code> file	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>bleepsetup</code>	
<b>Options</b>	<code>-f</code>	Properties file (silent mode)
	<code>-i</code>	Mode: {swing, console, recorderui, silent} Default: swing
	<code>-g</code>	Generate sample properties file
<b>Examples</b>	To run:	
	<code>arcsight bleepsetup</code>	

## changepassword

<b>Description</b>	Utility to change obfuscated passwords in properties files. The utility prompts for the new password at the command line	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>changepassword -f file -p property_name</code>	
<b>Options</b>	<code>-f file</code>	Properties file, such as <code>config/server.properties</code>
	<code>-p property_name</code>	Password property to change, such as <code>server.privatekey.password</code>

<b>Examples</b>	To run:
	<code>arcsight changepassword</code>

## checklist

<b>Description</b>	ArcSight Environment Check. Used internally by the installer.
	Right JRE, supported OS, connected to supported Database,
	Can run from Connector, Database, or Manager.

## console

<b>Description</b>	Run the ArcSight Console	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>console [-i] [options]</code>	
<b>Options</b>	<code>-ast file</code>	
	<code>-debug</code>	
	<code>-i</code>	
	<code>-imageeditor</code>	
	<code>-laf style</code>	Look and feel style: metal, plastic, plastic3d
	<code>-p password</code>	Password
	<code>-port</code>	Port to connect to Manager (default: 8443)
	<code>-redirect</code>	
	<code>-relogin</code>	
	<code>-server</code>	Manager host name
	<code>-slideshow</code>	
	<code>-theme</code>	
	<code>-timezone tz</code>	Timezone: such as "GMT" or "GMT-8:00"
	<code>-trace</code>	Log all Manager calls
	<code>-u name</code>	User name
<b>Examples</b>	To run the console:	
	<code>arcsight console</code>	

## consolesetup

<b>Description</b>	Run the ArcSight Console Configuration Wizard to reconfigure an existing installation	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>consolesetup [-i mode] [-f file] [-g]</code>	
<b>Options</b>	<code>-i mode</code>	Mode: <code>console</code> , <code>silent</code> , <code>recorderui</code> , <code>swing</code>
	<code>-f file</code>	Log file name (properties file in <code>-i silent</code> mode)
	<code>-g</code>	Generate sample properties file for <code>-i silent</code> mode
<b>Examples</b>	<p>To change some console configuration options:</p> <pre>arcsight consolesetup</pre>	

## database init

<b>Description</b>	Initializes the database. Use this utility to restart the ArcSight Database Configuration Wizard if you exit it before configuring all options or to re-initialize Oracle at a later date	
<b>Applies to</b>	Database	
<b>Syntax</b>	<code>database init</code>	
<b>Options</b>	<code>-p</code>	Enables you to install Enterprise Manager and set partition management parameters
<b>Examples</b>	<p>To initialize the database</p> <pre>arcsight database init</pre>	

## database pc

<b>Description</b>	Partition configuration utility	
<b>Applies to</b>	Database	
<b>Syntax</b>	<code>database pc</code>	
<b>Options</b>	<code>-d db_type</code>	Database type: <code>oracle</code> , <code>db2</code>
	<code>-i mode</code>	Mode: <code>silent</code>
	<code>-f file</code>	Properties filename. Required in <code>-i silent</code> mode
	<code>-g</code>	Generate the SQL scripts
	<code>-s</code>	Generate a sample properties file for use in <code>-i silent</code> mode

	<code>-x</code>	Execute the existing SQL scripts
	<code>-p</code>	Run this command in expert mode.  If the statistics updates are timing out and the event rate is very high, then the sample size should be reduced to 0.1. Using the <code>-p</code> option with this command opens the wizard and allows you to change the sample size.
<b>Examples</b>	To configure your database partition:  <code>arcsight database pc</code>	

## database pm

<b>Description</b>	Partition management tool	
<b>Applies to</b>	Database (Partition Manager)	
<b>Syntax</b>	<code>database pm</code>	
<b>Options</b>	<code>-cn command-name</code>	This is a required parameter.  Name of command you want to issue on the Partition Manager. One of: <ul style="list-style-type: none"> <li>manage</li> <li>compress</li> <li>update</li> </ul>
	<code>-c config</code>	The default configuration file to use ( <code>config/server.defaults.properties</code> )
	<code>-i invocation-mode</code>	The invocation mode. Use one of: <ul style="list-style-type: none"> <li>remote</li> <li>standalone</li> </ul>
	<code>-m manager-name</code>	The hostname or IP address of the ArcSight Manager
	<code>-p password</code>	The admin password for ArcSight Manager
	<code>-pc custom-configuration-file</code>	The custom configuration file to use ( <code>config/database.properties</code> )
	<code>-pn partition-name</code>	name of partitions for which statistics are to be updated
	<code>-port Manager-port</code>	port number of ArcSight Manager (8443)
	<code>-u user-name</code>	The admin user name for ArcSight Manager (usually admin)
	<code>-h</code>	help. Get help for this command
<b>Examples</b>	<code>arcsight database pm -cn Manage -m linux53_64_45sp3 -u admin -p arcsight</code>	

## database xts

<b>Description</b>	Extend the ArcSight Database Tablespaces. (This is a convenience tool; If you have the full Oracle license, you can optionally use Enterprise Manager or SQL*Plus.)
<b>Applies to</b>	Database
<b>Syntax</b>	<code>database xts</code>
<b>Options</b>	None
<b>Examples</b>	To extend your database space: <code>arcsight database xts</code>

## dbcheck

<b>Description</b>	Gathering information and statistics about the current ArcSight Database instance, such as the data to index size ratio
<b>Applies to</b>	Database
<b>Syntax</b>	<code>dbcheck</code>
<b>Options</b>	None
<b>Examples</b>	<code>arcsight dbcheck</code>

## dbview-generator

<b>Description</b>	Utility that generates database views based on the fields of a fieldset. Field sets are named subsets chosen from the available attributes of an event. To create a new field set or to see the existing ones, go to the <b>Active Channels</b> resource tree and click the <b>Field Sets</b> tab										
<b>Applies to</b>	Manager, Database										
<b>Syntax</b>	<code>dbview-generator -f fieldset -m manager -n view_name -p password -u user_name</code>										
<b>Options</b>	<table><tr><td><code>-f fieldset</code></td><td>URI of the fieldset from which you want to generate the database view</td></tr><tr><td><code>-m manager</code></td><td>Name of the Manager</td></tr><tr><td><code>-n view_name</code></td><td>Name for the view</td></tr><tr><td><code>-u user_name</code></td><td>User name to connect to the Manager</td></tr><tr><td><code>-p password</code></td><td>Password for the user_name</td></tr></table>	<code>-f fieldset</code>	URI of the fieldset from which you want to generate the database view	<code>-m manager</code>	Name of the Manager	<code>-n view_name</code>	Name for the view	<code>-u user_name</code>	User name to connect to the Manager	<code>-p password</code>	Password for the user_name
<code>-f fieldset</code>	URI of the fieldset from which you want to generate the database view										
<code>-m manager</code>	Name of the Manager										
<code>-n view_name</code>	Name for the view										
<code>-u user_name</code>	User name to connect to the Manager										
<code>-p password</code>	Password for the user_name										

<b>Examples</b>	To generate a database view containing fields in the Standard field set:	
	<pre>dbview-generator -f "/All Field Sets/ArcSight System/Active Channels/Standard" -m mymanager -n dv_view_standard -p mypassword -u myuser</pre>	
	To retrieve the data from the view you generated run the following command in SQL:	
	<pre>select * from db_view_standard</pre>	

## deploylicense

<b>Description</b>	Install a new ArcSight license file. The Manager may be running; it will detect the new license file automatically	
<b>Applies to</b>	Manager	
<b>Syntax</b>	deploylicense file	
<b>Options</b>	-f file	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
	-i mode	Mode: console, silent, recorderui, swing
<b>Examples</b>	<p>To deploy a new license:</p> <pre>arcsight deploylicense</pre>	

## downloadcertificate

<b>Description</b>	Wizard for importing certificates	
<b>Applies to</b>	Manager	
<b>Syntax</b>	downloadcertificate	
<b>Options</b>	-i mode	Mode: console, silent, recorderui, swing
	-f file	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
<b>Examples</b>	<p>To run:</p> <pre>arcsight downloadcertificate</pre>	

## dropSLPartitions

<b>Description</b>	Utility for dropping old Session List partitions	
<b>Applies to</b>	Database	
<b>Syntax</b>	<code>dropSLPartitions</code>	
<b>Options</b>	<code>-d retentionDays</code>	Number of days to retain data
	<code>-m manager</code>	The ArcSight Manager to communicate with
	<code>-p password</code>	<b>(Optional)</b> The password to log in with
	<code>-u username</code>	The user name used for logging in
	<code>-p port</code>	<b>(Optional)</b> The port used for communication (8443 by default)
	<code>-h</code>	(Optional) Get help for this command
<b>Examples</b>	To run:	
	<code>arcsight dropSLPartitions</code>	

## exceptions

<b>Description</b>	Search for logged exceptions in ArcSight log files	
<b>Applies to</b>	Manager, Console, SmartConnectors	
<b>Syntax</b>	<code>exceptions logfile_list [options] [path to the log file]</code>	
	The path to the log file must be specified relative to the current working directory.	
<b>Options</b>	<code>-x</code>	Exclude exceptions/errors that contain the given string. Use @filename to load a list from a file.
	<code>-i</code>	Include exceptions/errors that contain the given string. Use @filename to load a list from a file.
	<code>-r</code>	Exclude errors.
	<code>-q</code>	Quiet mode. Does not display exceptions/errors on the screen.
	<code>-e</code>	Send exceptions/errors to the given email address.
	<code>-s</code>	Use a non-default SMTP server. Default is <code>bynari.sv.arcsight.com</code> .
	<code>-u</code>	Specify a mail subject line addition, that is, details in the log.
	<code>-n</code>	Group exceptions for readability.



	<code>-l</code>	Show only exceptions that have no explanation.
	<code>-p</code>	Suppress the explanations for the exceptions.
<b>Example</b>	To run:	
	<pre>arcsight exceptions /opt/home/arcsight/manager/logs/default/server.log*</pre>	

## execproc


<b>Description</b>	Process Executor tool. Used on Unix platforms to execute shell commands	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>execproc</code>	
<b>Options</b>	None	
<b>Examples</b>	To run:	
	<code>arcsight execproc</code>	

## execprosvc

<b>Description</b>	Start or stop the Process Executor as a service	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<pre>execprosvc cmd [-wrapperConfig file] [initialHeap maxHeap]</pre>	
<b>Options</b>	<code>-c</code>	Console mode
	<code>-i</code>	Install service
	<code>initialHeap</code>	Initial heap memory size, in MB. (Default: 128)
	<code>maxHeap</code>	Maximum heap memory size, in MB. (Default: 512)
	<code>-q</code>	Stop service (quit)
	<code>-r</code>	Remove service
	<code>-s</code>	Start service
	<code>-wrapperConfig file</code>	

	To install a process called 'proc:'
<b>Examples</b>	<code>arcsight execprocsvc proc -i</code>
	To run the installed process with a maximum of 1GB of memory:
	<code>arcsight execprocsvc proc -s 128 1024</code>

## export\_system\_tables

<b>Description</b>	Utility to export your database tables. Upon successful completion the utility generates two files: a temporary parameter file and the actual database dump file, <code>arcsight.dmp</code> which is placed in the database's <code>&lt;ARCSIGHT_HOME&gt;/tmp</code> .	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>export_system_tables username password Mysqlname</code>	
<b>Options</b>	<code>username</code>	Oracle database username
	<code>password</code>	Password for the Oracle database user
	<code>Mysqlname</code>	Name of the Mysql database from which you are exporting the system tables
	<code>TNSname</code>	Name specified in <code>tnsnames.ora</code> for the database from which you are exporting the system tables
	<code>-s</code>	include session list tables
<b>Examples</b>	To run:	
	<code>arcsight export_system_tables &lt;username&gt;/&lt;password&gt;@&lt;TNS name&gt;</code>	
	<code>arcsight export_system_tables &lt;ArcSight username&gt; &lt;ArcSight password&gt; &lt;Mysql databasename&gt;</code>	
	<b>Note:</b>	
	When running the <code>export_system_tables</code> command, you may see an warning message in your command prompt or shell console window saying "Exporting questionable statistics". You can safely ignore this warning. This warning occurs when you export the table data with its related optimizer statistics and Oracle cannot verify the validity of these statistics.	
 <b>Note</b>	If you are using ESM v5.0 SP1 patch 2 on an Oracle 10.2.0.4 database, you might get the following error message.	
	"ORA-39071: Value for TABLES is badly formed."	
	Check to see if your Oracle compatibility is set to 10.2.0.1. If it is, set it to 10.2.0.4 and try again.	

## flexagentwizard

<b>Description</b>	Wizard-like tool to generate simple ArcSight FlexConnectors
<b>Applies to</b>	SmartConnectors
<b>Syntax</b>	<code>flexagentwizard</code>
<b>Options</b>	None
<b>Examples</b>	To run: <code>arcsight flexagentwizard</code>

## groupconflictingassets

<b>Description</b>	Tool that groups asset resources with common attribute values. Group Conflicting Attribute Assets Tool. Assets can have conflicting IP addresses or host names within a zone	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>groupconflictingassets</code>	
<b>Options</b>	<code>-c</code>	Clean (delete the contents of) the group to receive links to assets before starting. (Default: false)
	<code>-m host</code>	Manager host name or address
	<code>-o name</code>	Name for group to receive links to assets which have conflicting attributes. (Default: "CONFLICTING ASSETS")
	<code>-p password</code>	Password
	<code>-port n</code>	Port to connect to Manager (Default: 8443)
	<code>-prot string</code>	Protocol { http   https } (Default: https)
	<code>-user name</code>	User name
<b>Examples</b>	To run: <code>arcsight groupconflictingassets</code>	

## idensesetup

<b>Description</b>	Wizard to configure iDefense appliance information on the Manager
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>idensesetup</code>
<b>Options</b>	None

<b>Examples</b>	To launch the iDefense Setup wizard:
	<code>idefensesetup</code>

---

## import\_system\_tables

<b>Description</b>	Utility to import database tables. The file you import from must be the one that export_system_tables utility created. This utility looks for the arcsight.dmp file in the database's <ARCSIGHT_HOME>.	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>import_system_tables &lt;old_arcsight_user&gt; &lt;new_arcsight_user&gt; &lt;password&gt; &lt;db_instance&gt; &lt;dump_file_path&gt; &lt;dump_file_name&gt;</code>	
<b>Options</b>	<code>old_arcsight_user</code>	The database username that was used to export system tables using the <code>export_system_tables</code> command.
	<code>new_arcsight_user</code>	The database username of the database to which you are importing system tables
	<code>password</code>	Password for the <code>import_username</code>
	<code>TNSname</code>	Name specified in <code>tnsnames.ora</code> for the database to which you are importing the system tables
<b>Examples</b>	To run:	
	<code>arcsight import_system_tables &lt;old_arcsight_user&gt; &lt;new_arcsight_user&gt; &lt;password&gt; &lt;db_instance&gt; &lt;dump_file_path&gt; &lt;dump_file_name&gt;</code>	

---

## initorcl

<b>Description</b>	Initializes the database.
	This command is deprecated. Use database init instead.
<b>Applies to</b>	Database

## keytool

<b>Description</b>	Runs Java Runtime Environment keytool utility to manage key stores	
<b>Applies to</b>	Manager, Console, SmartConnectors	
<b>Syntax</b>	<code>keytool -store name</code>	
<b>Options</b>	<code>-store name</code>	<b>(Required)</b> Specific store { managerkeys   managercerts   clientkeys   clientcerts   ldapkeys   ldapcerts   webkeys   webcerts }
		<b>(original options)</b> All options supported by the JRE keytool utility are passed along. Use arcsight keytool
	<code>-help</code>	For a list of help topics, or see Java documentation
<b>Examples</b>	To view Console key store:	
	<code>arcsight keytool -store clientkeys</code>	

## keytoolgui

<b>Description</b>	Graphical user interface tool for manipulating key stores and certificates	
<b>Applies to</b>	Manager, Console	
<b>Syntax</b>	<code>keytoolgui</code>	
<b>Options</b>	None	
<b>Examples</b>	To run:	
	<code>arcsight keytoolgui</code>	

## kickbleep

<b>Description</b>	Runs a simple, standardized test using the bleep utility	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>kickbleep</code>	
<b>Options</b>	<code>-f</code>	Properties file (silent mode)

	<code>-g</code>	Generate sample properties file
	<code>-i</code>	Mode: {swing, console, recorderui, silent} Default: swing
<b>Examples</b>	To run: <code>arcsight kickbleep</code>	

## listsubjectdns

<b>Description</b>	Display subject distinguished names (DN) from a key store	
<b>Applies to</b>	Manager, SmartConnectors	
<b>Syntax</b>	<code>listsubjectdns</code>	
<b>Options</b>	<code>-store name</code>	Specific store { managerkeys   managercerts   clientkeys   clientcerts   ldapkeys   ldapcerts } (Default: clientkeys.)
<b>Examples</b>	To list Distinguished Names in the Console key store: <code>arcsight listsubjectdns</code>	

## logfu

<b>Description</b>	Graphical tool for analyzing log files.	
<b>Applies to</b>	Manager (See also agent logfu.)	
<b>Syntax</b>	<code>logfu {-a   -c   -m} [options]</code>	
<b>Options</b>	<code>-a</code>	Analyze SmartConnector logs
	<code>-c</code>	Analyze Console logs
	<code>-f timestamp</code>	From time
	<code>-i</code>	Display information about the log files that will be analyzed
	<code>-l timespec</code>	Analyze only the specified time (Format: <time>{smhd}) Examples: 1d = one day, 4h = four hours
	<code>-m</code>	Analyze Manager logs
	<code>-mempercent n</code>	Percent of memory messages to consider for plotting. (Default: 100)
	<code>-noex</code>	Skip exception processing
	<code>-noplot</code>	Skip the plotting
	<code>-t timestamp</code>	To time

<b>Examples</b>	To analyze Manager logs for the last 12 hours: <code>arcsight logfu -m -l 12h</code>
-----------------	-----------------------------------------------------------------------------------------

## manager

<b>Description</b>	Runs the ArcSight Manager in command line mode (not as a service)
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>manager</code>
<b>Options</b>	None
<b>Examples</b>	To run the ArcSight Manager: <code>arcsight manager</code>

## managerinventory

<b>Description</b>	Display configuration information about the installed Manager	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>managerinventory</code>	
<b>Options</b>	<code>-a filter</code>	Attribute filter. Default: ""
	<code>-f filter</code>	Object filter. Default: "Arcsight: *"
	<code>-m host</code>	Manager host name or address
	<code>-o op</code>	Operation {list, show}. Default is list
	<code>-out file</code>	Output filename. Default is stdout
	<code>-password pwd</code>	Password
	<code>-port n</code>	Port to connect to Manager (Default: 8443)
	<code>-prot string</code>	Protocol { http   https } (Default: https)
	<code>-user name</code>	User name
<b>Examples</b>	To run: <code>arcsight managerinventory</code>	

## manager-no-wrapper

<b>Description</b>	Run the Manager without automatic restart in case of fatal errors. (See manager for options.)
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>manager-no-wrapper</code>
<b>Options</b>	None
<b>Examples</b>	To run the manager without automatic restart:  <code>arcsight manager-no-wrapper</code>

## manager-reload-config

<b>Description</b>	Load the <code>server.defaults.properties</code> and <code>server.properties</code> files on the Manager
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>arcsight manager-reload-config</code>
<b>Options</b>	<div> <div><code>-diff</code></div> <div>Displays the difference between the properties the Manager is currently using and the properties that this command will load</div> </div> <div> <div><code>-as</code></div> <div>Forces the command to load properties that can be changed without restarting the Manager. The properties that require a Manager restart are updated in the <code>server.properties</code> but are not effective until the Manager is restarted</div> </div> <div> <div><code>-t updateTimeout</code></div> <div>Number of seconds after which the <code>manager-reload-config</code> command stops trying to load the updated properties file on the Manager</div> </div>
<b>Examples</b>	<p>To reload config:</p> <p><code>arcsight manager-reload-config</code></p> <p>To view the differences between the properties the Manager is currently using and the properties that this command will load:</p> <p><code>arcsight manager-reload-config -diff</code></p>

## managersetup

<b>Description</b>	Run the ArcSight Manager Configuration Wizard
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>managersetup -i console</code>
<b>Options</b>	<code>-i mode</code> Mode: console, silent, recorderui, swing



	<code>-f file</code>	Log file name (properties file in <code>-i</code> silent mode)
	<code>-g</code>	Generate sample properties file for <code>-i</code> silent mode
<b>Examples</b>	To run: <code>arcsight managersetup</code>	

## managerstop

<b>Description</b>	Stop the ArcSight Manager whether it is in service or command line mode	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>managerstop</code>	
<b>Options</b>	None	
<b>Examples</b>	To stop the Manager service: <code>arcsight managerstop</code>	

## managersvc

	Start, stop, install, or uninstall the ArcSight Manager as a service.	
<b>Description</b>	<b>Note:</b> The start option does not work on Windows. To start Manager as a service on Windows, follow instructions in <a href="#">Chapter 1, Basic Administration Tasks, on page 9</a> .	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>managersvc {start   stop   restart   status   dump}</code>	
<b>Options</b>	None	
<b>Examples</b>	To start the Manager service (only on non-Windows platforms): <code>arcsight managersvc start</code>	

## managerthreaddump

<b>Description</b>	Script to dump the Manager's current threads	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>managerthreaddump</code>	
<b>Options</b>	None	
<b>Examples</b>	To run: <code>arcsight managerthreaddump</code>	

## managerup

<b>Description</b>	Get the current state of the Manager. Returns 0 if the Manager is running and reachable. Returns 1 if not
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>managerup</code>
<b>Options</b>	None
<b>Examples</b>	To check that the Manager is up, running, and accessible: <code>arcsight managerup</code>

## monitor

<b>Description</b>	Tool used in conjunction with Network Management Systems	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>monitor</code>	
<b>Options</b>	<code>-a filter</code>	Attribute filter. Default: ""
	<code>-append</code>	Append to output file instead of overwriting (Default: false)
	<code>-f filter</code>	Object filter. Default: "Arcsight: *"
	<code>-m host</code>	Manager host name or address
	<code>-o op</code>	Operation {list, show}. Default is list
	<code>-out file</code>	Output filename for management service information. Default is stdout
	<code>-p pwd</code>	Password
	<code>-sanitize</code>	Sanitize IP address and host names (Default: false)
	<code>-u name</code>	User name
<b>Examples</b>	To run: <code>arcsight monitor</code>	

## netio

<b>Description</b>	Primitive network throughput measurement utility
<b>Applies to</b>	Manager
<b>Syntax</b>	<code>netio</code>

<b>Options</b>	<code>-c</code>	Client mode (Default: false)
	<code>-n host</code>	Host to connect to (Client mode only)
	<code>-p port</code>	Port (Default: 9999)
	<code>-s</code>	Server mode
<b>Examples</b>	To run:	
	<code>arcsight netio</code>	

## package

	Import or export resources (users, rules, and so on) to or from one or more XML files.	
<b>Description</b>	Use this command instead of the archive command.	
	<b>Note:</b> Some functionality for this command are available from the GUI only	
<b>Applies to</b>	Manager, Database, Console	
<b>Syntax</b>	<pre>package -action &lt;action-to-be-taken&gt; -package &lt;package URI&gt; -f &lt;package-file&gt;</pre>	
<b>Options</b>	- action action	Creates a new package based upon one or more packages that you specify. The possible actions include <code>bundle</code> , <code>convertarchives</code> , <code>export</code> , <code>import</code> , <code>install</code> , <code>uninstall</code> . The default is <code>export</code>
	-config config file	The primary configuration file to use. Default is <code>config/server.defaults.properties</code>
	-convertbaseuri baseuri	The base URI for packages that are converted from archives. This option is only used in conjunction with the <code>-action convertarchives</code> option
	-f packagefile-location	The location of the package bundle file. File name paths can be absolute or relative. Relative paths are relative to <code>&lt;ARCSIGHT_HOME&gt;</code>
	-m manager	The Arcsight Manager to communicate with
	-password password	<b>(Optional)</b> The password with which to log in to the Manager
	-package packagerefs	The URI(s) of the package(s). This option is used in conjunction with <code>-action install</code> and <code>-action uninstall</code> in order to list which packages to operate upon
	-pc privateConfig	This configuration file will override the <code>server.defaults.properties</code> file. The default location is <code>config/server.properties</code>
	-pkcs11	Use this option when authenticating with a PKCS#11 provider. For example,  <pre>arcsight package -m &lt;hostname&gt; -pkcs11 -f &lt;file path&gt;</pre>
	-port port	The port to use for communication. The default port used is 8443
	-source sourcefile	The source file. This is used in conjunction with the <code>-f</code> command which specifies an output file
	-u username	The user name used for logging in to the Manager

---

<code>-standalone</code>	Operate directly on the Database not the Manager
--------------------------	--------------------------------------------------

---

To convert a previously archived package:

```
arcsight package -action convertarchives -convertbaseuri
"/All Packages/Personal/Mypackage" -source sourcefile.xml
-f packagebundle.arb
```

To install a package:

```
arcsight package -action install -package "/All
Packages/Personal/Mypackage" -u username -p password -m
managename
```

To uninstall a package:

```
arcsight package -action uninstall-package "/All
Packages/Personal/Mypackage" -standalone -config
/config/server.defaults.properties -pc
/config/server.properties
```

To import a package through the Manager:

```
arcsight package -action import -f packagebundle.arb -u
username -p password -m managename
```

To export a package:

### Examples

```
arcsight package -action export -package "/All
Packages/Personal/Mypackage" -f packagebundle.arb -u
username -p password -m managename
```

To export multiple packages:

```
arcsight package -action export -package "/All
Packages/Personal/PackageOne" -package "/All
Packages/Personal/PackageTwo" -f packagebundle.arb -u
username -p password -m managename
```

To export packages in a standalone mode (directly from the database) Make sure that the ArcSight Manager is not running:

```
arcsight package -action export -package "/All
Packages/Personal/Mypackage" -f packagebundle.arb -u
username -p password -standalone -config
server.default.properties -pc server.properties
```

To combine xml files from multiple packages into one package:

```
arcsight package -action bundle -f myPkgNew.arb -source
chnpkg.xml -source filterpkg.xml -source rulepkg.xml
```

In the above example, `chnpkg.xml`, `filterpkg.xml`, and `rulepkg.xml` files are extracted from their respective packages and will be bundled in one package bundle called `myPkgNew.arb`.

---

## portinfo

<b>Description</b>	Script used by the portinfo tool of the Console. Displays common port usage information for a given port	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>portinfo port</code>	
<b>Options</b>	<code>port</code>	Port number
<b>Examples</b>	<p>To run:</p> <pre>arcsight portinfo</pre>	

## querytuner

<b>Description</b>	<p>A troubleshooting tool that generates explain plans for all queries within ArcSight ESM, and helps evaluate whether hints may improve the performance of some queries. This tool pulls explain plans for all the queries used by reports and trends and looks for ones that will execute inefficiently without database hints.</p> <p>All findings are logged in the file Manager's <code>&lt;ARCSIGHT_HOME&gt;/logs/query-tuner.log</code>.</p> <p>Run this tool from the Manager's <code>bin</code> directory either in a standalone mode (without the Manager running) or you can run it while the Manager is running.</p>	
<b>Applies to</b>	Database, Manager, Console	
<b>Syntax</b>	<code>arcsight querytuner -m analyze -uri &lt;uri_for_the_query&gt;</code>	
<b>Options</b>	<code>-m analyze</code>	To analyze a query
	<code>-d &lt;query_duration&gt;</code>	<b>Optional parameter.</b> <code>query_duration</code> is the time duration, for example, 1h, 2h, 1d, to be used while running the queries
	<code>-t &lt;timeout&gt;</code>	<b>Optional parameter.</b> <code>timeout</code> is the number of seconds after which a slow running query will timeout. If you provide this value, performance will be measured if and when a good hint is found
	<code>-uri &lt;uri&gt;</code>	<b>Optional parameter.</b> <code>uri</code> is the URI of the query
	<code>-h</code>	Help for this command, for example, <code>./arcsight querytuner -h</code>

Examples	<p>To analyze all the queries</p> <pre>bin&gt;arcsight querytuner -m analyze</pre> <p>To analyze all queries and measure performance if a hint helps, <code>-t</code> is the timeout to be used while executing the query:</p> <pre>bin&gt;arcsight querytuner -m analyze -t 300000</pre> <p>To analyze a single query:</p> <pre>bin&gt;arcsight querytuner -m analyze -uri &lt;uri_for_the_query&gt;</pre> <p>For example,</p> <pre>bin&gt; arcsight querytuner -m analyze -uri "/All Queries/ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Business Role/Business Role - Successful Attacks"</pre> <p>This will tell you if any hint may potentially help. You should see the message "Hint that Helped=&lt;the_actual_hint&gt;" in the query-tuner.log file to look for a hint that might potentially help.</p> <p>Open the <code>query-tuner.log</code> file. For every Query at the end of the query report look for the keyword "hasBadPattern=true" followed by "Hint that Helped=&lt;the_actual_hint&gt;" or sometimes you will see "No hints could be found for this pattern."</p> <p>Please contact Customer support when you see "hasBadPattern=true" followed by "No hints could be found for this pattern." Be prepared to provide the querytuner log and the package export of the query.</p> <p>Once you run the Query Tuner tool and see that a hint has helped for a particular query, you can install the hint on the Manager from the ArcSight Console. Refer to the Console's online help for information on how to do so.</p>
	<p><b>Note:</b> Please contact ArcSight Customer Support before applying any hints received by running the Query Tuner.</p> <p>Once you run the Query Tuner tool and see that a hint has helped for a particular query, you can add the hint to the query as follows:</p> <ol style="list-style-type: none"> <li>1 In the Console's <code>&lt;ARCSIGHT_HOME&gt;/current/config/console.properties</code> file, set the following property: <pre>database.hint.editable=true</pre> </li> <li>2 Restart the Console if it is running.</li> <li>3 Open the <code>query-tuner.log</code> file located in the Manager's <code>&lt;ARCSIGHT_HOME&gt;/logs</code> directory.</li> <li>4 Scan through the file and locate the query URI. Copy the actual hint in the line "Hint that Helped=&lt;the_actual_hint&gt;" located below the query URI. Make sure not to copy the words "Hint that Helped="</li> <li>5 In the ESM Console Navigator, open the <b>Reports</b> resource.</li> <li>6 Click on the <b>Queries</b> tab to bring it forward.</li> <li>7 Follow the URI for the query for which you want to apply the hint, right-click it and select <b>Edit Query</b>.</li> <li>8 In the Inspect/Edit panel, paste the hint you copied in <a href="#">Step 4</a> in the Database Hint box (the actual hint).</li> </ol>

### Applying a Hint to a Query

## reenableuser

<b>Description</b>	Re-enable a disabled user account	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>reenableuser username</code>	
<b>Options</b>	<code>username</code>	The name of the user resource to re-enable
<b>Examples</b>	To re-enable a disabled user: <code>arcsight reenableruser &lt;username&gt;</code>	

## refcheck

<b>Description</b>	Resource reference checker	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>refcheck</code>	
<b>Options</b>	None	
<b>Examples</b>	To run: <code>arcsight refcheck</code>	

## regex

<b>Description</b>	Graphical tool for regex-based FlexConnectors	
<b>Applies to</b>	SmartConnectors	
<b>Syntax</b>	<code>regex</code>	
<b>Options</b>	None	
<b>Examples</b>	To run: <code>arcsight regex</code>	

## replayfilegen

<b>Description</b>	Wizard for creating security event data files ("replay files") that can be run against a Manager for testing, analysis, or demonstration purposes.  <b>Note:</b> This is a client side command only and should be executed from the Console's <code>ARCSIGHT_HOME/bin</code> directory.	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>replayfilegen -m mgr [options]</code>	



<b>Options</b>	<code>-f file</code>	Log file name (properties file in <code>-i</code> silent mode)
	<code>-g</code>	Generate sample properties file for <code>-i</code> silent mode
	<code>-i mode</code>	Mode: console, silent, recorderui, swing
<b>Examples</b>	Run from the Console's <code>&lt;ARCSIGHT_HOME&gt;/bin</code> directory:	
	<code>arcsight replayfilegen</code>	
	To run in console mode:	
	<code>arcsight replayfilegen -i console</code>	

## rescheck

<b>Description</b>	Verify the integrity of the resource database	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>rescheck</code>	
<b>Options</b>	<code>-f file_list</code>	Archive file names (Default: Read the database, not archives)
	<code>-config file</code>	Primary configuration file. Default: <code>config/server.defaults.properties</code>
	<code>-pc</code>	Private configuration file
	<code>-amiss</code>	Only check for resources that are in the archive, but which are missing from the Database
<b>Examples</b>	To run:	
	<code>arcsight rescheck</code>	

## resetpwd

<b>Description</b>	Wizard to reset a user's password and optionally notify the user of the new password by e-mail	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>resetpwd</code>	
<b>Options</b>	<code>-f file</code>	Log file name (properties file in <code>-i</code> silent mode)
	<code>-g</code>	Generate sample properties file for <code>-i</code> silent mode
	<code>-i mode</code>	Mode: console, silent, recorderui, swing
	<code>-h</code>	Display command help

---

**Examples**

To reset a user's password:

```
arcsight resetpwd
```

---

## restorearchives

This tool allows you to load archives from an older ArcSight Express installation to a new one. The loaded archives from the older installation are loaded as archives in DEACTIVATED state. By activating them, you can load the events and search through them as you would for an archive that was done from the newer installation. The system does not differentiate between the archives loaded from a different installation and the ones created daily locally.

### Description

#### Notes:

- If you override the archive root path, then the files are not copied over to the default archive location. Hence deleting those files will make the archive unusable. The space used by these archive is not shown in the "Archive Jobs" administration page.
- Loading events from two installations to the local installation is not recommended.

### Applies to

Database

### Syntax

```
/opt/arcsight/logger/current/arcsight/bin/arcsight
restorearchives
```

### Options

`-r <root>`

Optional Parameter.

The root of the directory that contains all archives to be imported. All archives should be sub-directories of this directory. If unspecified the tool loads archives from the default archive location,  
`/opt/arcsight/logger/data/archives`

`-i interactive`

Interactive mode. Confirmation will be required before loading each archive. Use this mode to selectively load a subset of the archives.

`-t test`

This option helps you validate the archives without actually loading them into the database.

`-C clear`

Clears all events and archives from the database, and then load the archives. This is required when the events loaded from a different ArcSight Express appliance clashes with the events present in the local appliance. This is useful when the tool skips some archives because of event ID clash, or archive clash. This tool will remove all events and archives from the local installation. Therefore, this option is most useful for a fresh ArcSight Express installation.

`-h help`

Help for this command

### Examples

To run:

```
arcsight restorearchives -C
```

## resvalidate

<b>Description</b>	Utility for checking whether there are any invalid resources in the database. The utility generates two reports called <a href="#">validationReport</a> (with .xml and .html extensions) that are written to the directory from which you run the <a href="#">resvalidate</a> command	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<a href="#">resvalidate</a>	
<b>Options</b>	<a href="#">-excludeTypes</a> <a href="#">&lt;exclude_resource</a> <a href="#">_names&gt;</a>	Resource type to exclude from being checked; for example, Rule, DataMonitor
		If specifying multiple resource types to exclude, use comma to separate them.
		Resource type – Rule, DataMonitor (comma separated)
	<a href="#">-out &lt;output_dir&gt;</a>	Output directory for validation report. If none is specified, the report is placed in the directory from which you run the <a href="#">resvalidate</a> command
	<a href="#">-persist [false   true]</a>	If a resource is found to be invalid, whether to mark it invalid or only report it as invalid. For example, a rule depends on a filter that is missing. When you run the <a href="#">resvalidate</a> command and <a href="#">-persist=false</a> , the rule will be reported as invalid but not marked invalid. However if <a href="#">-persist=true</a> , the rule will be marked as invalid.
		Default: <a href="#">persist=false</a> .
<b>Examples</b>	To run:  <a href="#">arcsight resvalidate</a>	

## ruledesc

<b>Description</b>	Rule description tool to fetch rules information. (Used by HPOVO.) Tool to monitor managed objects in the ArcSight Manager	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<a href="#">ruledesc -t {ovo uri} -i info [options]</a>	
<b>Options</b>	<a href="#">-t type</a>	<b>(Required)</b> Type: { ovo   uri }
	<a href="#">-i info</a>	<b>(Required)</b> Info (depends on type).
	<a href="#">-m host</a>	Manager host name or address
	<a href="#">-p pwd</a>	Password
	<a href="#">-port</a>	Port for Manager. Default: 8443

`-prot` Protocol {http | https}. Default: https

`-u name` User name

---

**Examples**

To run:

`arcsight ruledesc`

---

## runcertutil

<b>Description</b>	<p>A wrapper launcher for the nss certutil tool used for managing certificates and key pairs. For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website.</p> <p><b>Note:</b> If you do not see any error or warning messages after <code>runcertutil</code> has run, it is an indication that the command completed successfully.</p>																				
<b>Applies to</b>	N/A																				
<b>Syntax</b>	<code>arcsight runcertutil</code>																				
<b>Options</b>	<table> <tr> <td data-bbox="571 598 603 625"><code>-A</code></td><td data-bbox="812 598 1166 625">Add a certificate to the database</td></tr> <tr> <td data-bbox="571 655 603 682"><code>-a</code></td><td data-bbox="812 655 1283 709">Use ASCII format or allow the use of ASCII format for input or output.</td></tr> <tr> <td data-bbox="571 739 783 808"><code>-v &lt;certificate_validity_in_months&gt;</code></td><td data-bbox="812 739 1315 993"> <p>Set the number of months a new certificate will be valid. You can use this option with the <code>-w</code> option which will set the beginning time for the certificate validity. If you do not use the <code>-w</code> option, the validity period begins at the current system time.</p> <p>If you do not specify the <code>-v</code> argument, the default validity period of the certificate is three months.</p> </td></tr> <tr> <td data-bbox="571 1022 783 1092"><code>-w &lt;beginning_offset_months&gt;</code></td><td data-bbox="812 1022 1315 1203">Set an offset from the current system time, in months, for the beginning of a certificate's validity period. Can be used when creating the certificate. Use a minus sign (-) to indicate a negative offset. If this argument is not used, the validity period begins at the current system time.</td></tr> <tr> <td data-bbox="571 1232 783 1302"><code>-n &lt;certificate_name&gt;</code></td><td data-bbox="812 1232 1315 1499"> <p>Alias for the certificate</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When generating a key pair on the Manager or ArcSight Web, it is mandatory to set the alias name to "mykey" (without the quotes)</li> <li>When importing a certificate, you can set the alias name to any name of your choice</li> </ul> </td></tr> <tr> <td data-bbox="571 1528 783 1598"><code>-t &lt;trust_attributes&gt;</code></td><td data-bbox="812 1528 1177 1556">Set the certificate trust attributes</td></tr> <tr> <td data-bbox="571 1627 783 1696"><code>-d &lt;certificate_database_dir&gt;</code></td><td data-bbox="812 1627 1203 1654">Directory of the certificate database</td></tr> <tr> <td data-bbox="571 1726 603 1753"><code>-i</code></td><td data-bbox="812 1726 1091 1753">Certificate import request</td></tr> <tr> <td data-bbox="571 1782 603 1810"><code>-L</code></td><td data-bbox="812 1782 1050 1810">List all the certificates</td></tr> <tr> <td data-bbox="571 1839 603 1866"><code>-r</code></td><td data-bbox="812 1839 963 1866">Encoding type</td></tr> </table>	<code>-A</code>	Add a certificate to the database	<code>-a</code>	Use ASCII format or allow the use of ASCII format for input or output.	<code>-v &lt;certificate_validity_in_months&gt;</code>	<p>Set the number of months a new certificate will be valid. You can use this option with the <code>-w</code> option which will set the beginning time for the certificate validity. If you do not use the <code>-w</code> option, the validity period begins at the current system time.</p> <p>If you do not specify the <code>-v</code> argument, the default validity period of the certificate is three months.</p>	<code>-w &lt;beginning_offset_months&gt;</code>	Set an offset from the current system time, in months, for the beginning of a certificate's validity period. Can be used when creating the certificate. Use a minus sign (-) to indicate a negative offset. If this argument is not used, the validity period begins at the current system time.	<code>-n &lt;certificate_name&gt;</code>	<p>Alias for the certificate</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When generating a key pair on the Manager or ArcSight Web, it is mandatory to set the alias name to "mykey" (without the quotes)</li> <li>When importing a certificate, you can set the alias name to any name of your choice</li> </ul>	<code>-t &lt;trust_attributes&gt;</code>	Set the certificate trust attributes	<code>-d &lt;certificate_database_dir&gt;</code>	Directory of the certificate database	<code>-i</code>	Certificate import request	<code>-L</code>	List all the certificates	<code>-r</code>	Encoding type
<code>-A</code>	Add a certificate to the database																				
<code>-a</code>	Use ASCII format or allow the use of ASCII format for input or output.																				
<code>-v &lt;certificate_validity_in_months&gt;</code>	<p>Set the number of months a new certificate will be valid. You can use this option with the <code>-w</code> option which will set the beginning time for the certificate validity. If you do not use the <code>-w</code> option, the validity period begins at the current system time.</p> <p>If you do not specify the <code>-v</code> argument, the default validity period of the certificate is three months.</p>																				
<code>-w &lt;beginning_offset_months&gt;</code>	Set an offset from the current system time, in months, for the beginning of a certificate's validity period. Can be used when creating the certificate. Use a minus sign (-) to indicate a negative offset. If this argument is not used, the validity period begins at the current system time.																				
<code>-n &lt;certificate_name&gt;</code>	<p>Alias for the certificate</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When generating a key pair on the Manager or ArcSight Web, it is mandatory to set the alias name to "mykey" (without the quotes)</li> <li>When importing a certificate, you can set the alias name to any name of your choice</li> </ul>																				
<code>-t &lt;trust_attributes&gt;</code>	Set the certificate trust attributes																				
<code>-d &lt;certificate_database_dir&gt;</code>	Directory of the certificate database																				
<code>-i</code>	Certificate import request																				
<code>-L</code>	List all the certificates																				
<code>-r</code>	Encoding type																				

<code>-o &lt;filename&gt;</code>	Output file name for new certificates or binary certificate requests. Be sure to use quotation marks around the file name if the file name contains spaces. If you do not specify a filename, by default, the output will be directed to standard output.
<code>-S</code>	Create a certificate to be added to the database
<code>-s &lt;subject&gt;</code>	Subject name
<code>-k &lt;key_type&gt;</code>	Type of key pair to generate
<code>-x</code>	Self signed
<code>-m &lt;serial_number&gt;</code>	Certificate serial number
<code>-v &lt;number_of_days&gt;</code>	Validity period in days, for example, use <code>-v 1825</code> to change the validity period to 5 years where 1825 is the number of days in 5 years.
<code>-V</code>	Check the validity of the certificate
<code>-n &lt;cert_name&gt;</code>	Certificate name
<code>-H</code>	Help on this tool
<b>Examples</b>	<p>To run:</p> <pre>arcsight runcertutil</pre>

## runmodutil

<b>Description</b>	<p>A wrapper launcher for the <code>modutil</code> nss cryptographic module utility.</p> <p>For more details on the <code>certutil</code> tool, you can visit the 'NSS Security Tools' page on the Mozilla website.</p>						
<b>Applies to</b>	N/A						
<b>Syntax</b>	<code>arcsight runmodutil</code>						
<b>Options</b>	<table> <tr> <td><code>-fips [true false]</code></td><td>Alias for the certificate</td></tr> <tr> <td><code>-dbdir &lt;path_to_directory&gt;</code></td><td>The security database directory</td></tr> <tr> <td><code>-H</code></td><td>Help on this tool</td></tr> </table>	<code>-fips [true false]</code>	Alias for the certificate	<code>-dbdir &lt;path_to_directory&gt;</code>	The security database directory	<code>-H</code>	Help on this tool
<code>-fips [true false]</code>	Alias for the certificate						
<code>-dbdir &lt;path_to_directory&gt;</code>	The security database directory						
<code>-H</code>	Help on this tool						
<b>Examples</b>	<p>To run:</p> <pre>arcsight runmodutil</pre>						

## runpk12util

<b>Description</b>	The pk12util allows you to export certificates and keys from your database and import them into nssdb. This is a wrapper launcher for the <code>pk12util</code> nss tool.	
	For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website.	
<b>Applies to</b>	N/A	
<b>Syntax</b>	<code>arcsight runpk12util</code>	
<b>Options</b>	<code>-d</code>	Path to your certificate directory (nssdb)
	<code>&lt;Certificate_directory&gt;</code>	
	<code>-i</code>	The name of the file to be imported
	<code>&lt;file_to_be_imported&gt;</code>	
	<code>-h</code>	Help on this tool
<b>Examples</b>	To run:	
	<code>arcsight runpk12util</code>	



## script

<b>Description</b>	Run a Python script	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>script -f script_file</code>	
<b>Options</b>	<code>-f file list</code>	The script(s) to run
	<code>-a args</code>	Command line arguments to pass to script
<b>Examples</b>	<p>To run a Python script:</p> <pre>arcsight script myScript.py</pre>	

## searchindex

<b>Description</b>	Utility that creates or updates the search index for resources in ArcSight Database.	
	<p>If you provide the credentials for the Manager, it automatically associates with the newly created or updated index. However, if you do not specify any credentials, you will have to manually configure the Manager to use the updated index.</p> <p><b>Note:</b> Supporting 50,000 actors will require a minimum of 2 GB heap size for this service. The value of the heap size needs to be modified in <code>&lt;ARCSIGHT_HOME&gt;/bin/scripts/searchindex.bat</code> and <code>&lt;ARCSIGHT_HOME&gt;/bin/scripts/searchindex.sh</code> files. The default value in these files is set to 1028m.</p>	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>searchindex -a action</code>	
<b>Options</b>	<code>-a action</code>	<p>Possible actions: <code>create</code>, <code>update</code>, or <code>regularupdate</code></p> <p><code>create</code>—Creates a new search index.</p> <p><code>update</code>—Updates all resources in the index that were touched since the last daily update was run. Although “update” is a scheduled task that runs daily, you can run it manually.</p> <p><code>regularupdate</code>—Updates all resources in the index that were touched since the last regular update was run. Although “regular update” is a scheduled task that runs every 5 minutes, you can run it manually.</p>
	<code>-m manager</code>	Name of the Manager
	<code>-p password</code>	Password for the user
	<code>-t time</code>	Time stamp that indicates starting when the resources should be updated

`-u user`

User name with which to log in to the Manager

---

**Examples**

To run:

`arcsight searchindex -a action`

---

## sendlogs

<b>Description</b>	Wizard to sanitize and send ArcSight log files to ArcSight for analysis. (This utility replaces the old 'packlogs' tool.)	
<b>Applies to</b>	Manager, Database, Console, SmartConnectors	
<b>Syntax</b>	<code>sendlogs</code>	
<b>Options</b>	<code>-f file</code>	Log file name (properties file in <code>-i</code> silent mode)
	<code>-g</code>	Generate sample properties file for <code>-i</code> silent mode
	<code>-i mode</code>	Mode: <code>console</code> , <code>silent</code> , <code>recorderui</code> , <code>swing</code>
	<code>-n num</code>	Incident number (Quick mode)
<b>Examples</b>	To run on all components except SmartConnectors:	
	<code>arcsight sendlogs</code>	
	To run on SmartConnectors:	
	<code>arcsight agent sendlogs</code>	

## tee

<b>Description</b>	Displays the output of a program and simultaneously writes that output to a file	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>-f filename</code>	
<b>Options</b>	<code>-a</code>	Append to the existing file
<b>Examples</b>	To run:	
	<code>arcsight tempca -i   arcsight tee sslinfo.txt</code>	

## tempca

<b>Description</b>	Inspect and manage demo certificates	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>tempca</code>	
<b>Options</b>	<code>-a alias</code>	Key store alias of the private key to dump
	<code>-ac</code>	Add the demo CA's certificate to the client truststore
	<code>-ap</code>	Create demo SSL key pair and add it to ArcSight Manager key store

<code>-dc</code>	Dump/export the demo CA's certificate to a file ( <code>demo.crt</code> ) for browser import
<code>-dpriv</code>	Dump private key from ArcSight Manager key store
<code>-f file</code>	Filename to write the demo CA's certificate to
<code>-i</code>	Display summary of current SSL settings
<code>-k n</code>	Key store: Manager (1) or Web Server (2)
<code>-n host</code>	Host name of the Manager (opt for the creation of a demo key pair)
<code>-nc</code>	No chain: Do not include certificate chain (option for creation of a demo key pair)
<code>-rc</code>	Reconfigure not to trust demo certificates. Removes the demo CA's certificate from the client truststore
<code>-rp</code>	Remove pair's current key pair from ArcSight Manager key store
<code>-v d</code>	Validity of the new demo certificate in days (Default: 365)

---

**Examples**

To run:  
`arcsight tempca`

---

## testdbconnection

<b>Description</b>	Test whether the database is up and running	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>testdbconnection -u username -p password</code>	
<b>Options</b>	<code>-u username</code>	<b>(Required)</b> User name of the ArcSight user in the database. Typically, arcsight
	<code>-p password</code>	<b>(Required)</b> Password of the ArcSight user in the database
	<code>-i instance</code>	Instance of the database. Default: arcsight
	<code>-p port</code>	Port to connect. Default: 1521
	<code>-s host</code>	Hostname of the machine on which database is located.  Default: localhost
	<code>-t dbtype</code>	Database type: oracle. Default: oracle
<b>Examples</b>	<code>testdbconnection -u arcsight -p password</code>	

## threaddumps

<b>Description</b>	Utility to extract and reformat thread dumps from Manager log files	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>threaddumps [file]</code>	
<b>Options</b>	None	
<b>Examples</b>	To run:	
	<code>arcsight threaddumps</code>	

## tproc

<b>Description</b>	Standalone Velocity template processor	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>tproc</code>	
<b>Options</b>	<code>-d file</code>	Definitions file
	<code>-Dname=value</code>	Defines
	<code>-h</code>	Display command help

<code>-l</code>	Keep log file
<code>-o file</code>	Output file
<code>-p file</code>	Properties file
<code>-t file</code>	Template file
<code>-v</code>	Verbose mode

---

**Examples**

To run:

```
arcsight tproc
```

---

## uninstallservice

<b>Description</b>	Wizard to uninstall service	
<b>Applies to</b>	Manager, ArcSight Web	
<b>Syntax</b>	<code>uninstallservice</code>	
<b>Options</b>	<code>-c component</code>	Component whose service will be uninstalled—Manager or Web
<b>Examples</b>	To run: <code>arcsight uninstallservice</code>	

## webserver

<b>Description</b>	Start the ArcSight Web server	
<b>Applies to</b>	ArcSight Web	
<b>Syntax</b>	<code>webserver</code>	
<b>Options</b>	<code>-c file</code>	Base configuration file
	<code>-host host</code>	Manager name or address
	<code>-p port</code>	Manager port
	<code>-pc file</code>	User configuration file
<b>Examples</b>	To start the ArcSight Web server: <code>arcsight webserver</code>	

## webserver-no-wrapper

<b>Description</b>	Start the ArcSight Web server without automatic restart	
<b>Applies to</b>	ArcSight Web	
<b>Syntax</b>	<code>webserver-no-wrapper</code>	
<b>Options</b>	<code>-ms mem</code>	Minimum memory
	<code>-mx mem</code>	Maximum memory
<b>Examples</b>	To start the ArcSight Web server without automatic restart: <code>arcsight webserver-no-wrapper</code>	

## webserversetup

<b>Description</b>	See <a href="#">runwebsetup</a> and <a href="#">websetup</a>
<b>Applies to</b>	ArcSight Web

## webserversvc

<b>Description</b>	Start, stop, restart, or install the ArcSight Web server as a service				
<b>Applies to</b>	ArcSight Web				
<b>Syntax</b>	<a href="#">webserversvc [options]</a> You can use the single letter options shown in brackets instead of entering the whole word on Windows only				
Options	Description	Windows	Solaris	Linux	AIX
<b>start or (-s)</b>	Start the service	No  (Command available but does not work)	Yes	Yes	Yes
<b>stop or (-q)</b>	Stop the service	Yes	Yes	Yes	Yes
<b>restart</b>	Restart the service	No	Yes	Yes	Yes
<b>status</b>	Check status of service	No	No	Yes	Yes
<b>install or (-i) &lt;initialHeap&gt; &lt;maxHeap&gt;</b>	Install the service  Optional parameters:  <a href="#">initialHeap</a> — Initial heap memory size, in MB. (Default: 128)  <a href="#">maxHeap</a> — Maximum heap memory size, in MB. (Default: 512)	Yes	No	No	No
<b>remove or (-r)</b>	Remove the service	Yes	No	No	No
<b>console or (-c)</b>	Console Mode	Yes	No	No	No
<b>Examples</b>	To start the ArcSight Web server as a service:  <a href="#">arcsight webserversvc start</a>				



## websetup

<b>Description</b>	Run the ArcSight Web Configuration Wizard
<b>Applies to</b>	ArcSight Web
<b>Syntax</b>	<code>websetup</code>
<b>Options</b>	None
<b>Examples</b>	To run the ArcSight Web Configuration Wizard: <code>arcsight websetup</code>

## whois

<b>Description</b>	Script used by the <code>whois</code> command of the console	
<b>Applies to</b>	Console	
<b>Syntax</b>	<code>whois [-p port] [-s host] target</code>	
<b>Options</b>	<code>-p port</code>	Server port
	<code>-s host</code>	Name or address of 'whois' server
	<code>target</code>	Name or address to lookup
<b>Examples</b>	To run: <code>arcsight whois</code>	



## Appendix B

# Troubleshooting

---

The following information may help solve problems that occur while operating the ArcSight system. In some cases, the solution can be found here or in specific ArcSight documentation, but ArcSight Customer Support is available if you need it.

If you intend to have ArcSight Customer Support guide you through a diagnostic process, please prepare to provide specific symptoms and configuration information. If you intend to do the initial diagnostic steps yourself, proceed through the following checklist systematically, trying each applicable item and noting the results for reference.

This appendix is divided into the following sections:

- [“General” on page 155](#)
- [“Query and Trend Performance Tuning” on page 158](#)
- [“SmartConnectors” on page 161](#)
- [“Console” on page 162](#)
- [“Manager” on page 164](#)
- [“ArcSight Web” on page 165](#)
- [“Database” on page 166](#)
- [“SSL” on page 167](#)

## General

### Report is empty or missing information.

Check that the user running the report has inspect (read) permission for the data being reported.

### Running a large report crashes the Manager.

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the ArcSight Manager to crash and restart. To prevent this scenario, you can set up the Manager to expose a special report parameter for generating the report in a separate process. The separate process has its own VM and heap, so the report is more likely to generate successfully. Even if the memory allocated is still not enough, the report failure will not crash the Manager.

This option must be set up on the Manager to expose it in the Console report parameters list. The steps are as follows:

- 1 On the ArcSight Manager in the `server.properties` file, set `report.canarchiveinseparateprocess=true`. (This will make a new report parameter available on the Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight ESM Console, open the report that you want to run in a separate process in the Report Editor, and click the **Parameters** tab. Set the parameter **Generate Report In Separate Process** to `true`.
- 4 Run the report. The report should run like a normal report, but it will not consume the resources of the Manager VM.

**Note**

Use this parameter only if you experience a Manager crash when running large reports such as the ones that contain tables with more than 500,000 rows and 4 or 5 columns per row.

---

## Reports that query over a large time range with complex joins take a long time to run.

You can expedite a report that queries over a large time range with complex joins if you set it to query with a full scan database hint. To set the query with full scan database hint, do this:

- 1 On the ArcSight Manager in the `server.properties` file, set `report.canquerywithfullscanhint=true`. (This will make a new report parameter available on the Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight ESM Console, open the report that you want to contain the full scan hint in the Report Editor, and click the **Parameters** tab. Set the parameter **Query with Full Scan Hint** to `true`.
- 4 Run the report.

**Note**

- 1 Use this parameter only in special circumstances if your organization has determined with the help of ArcSight support or professional services that it is appropriate.
  - 2 If a report is saved with the parameter set to "`true`", the full database optimization hint is applied even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to false later on.
  - 3 When the property `report.canquerywithfullscanhint` is set to "`true`", the report uses the `FULL_SCAN` hint in the SQL queries it generates to query the database. The content of the report does not change, but the queries logged in `server.report.log` contain the hint. The main benefit of querying the database with the `FULL_SCAN` hint is that it can significantly reduce the runtime for SQL queries that query over events within a large time range and contain complex joins.
- 

## Some Asian language fonts appear mangled when generating reports in PDF

This problem occurs because some Asian language fonts that are truetype fonts are not supported directly by versions of Adobe Reader earlier than version 8.0. In order to work around this, each truetype font must be mapped to an opentype font supported in Adobe

Reader 8.0. ArcSight provides this mapping in the `<ARCSIGHT_HOME>/il8n/server/reportpdf_config_<locale>.properties` file. You have the option to change the default mapping of any truetype font to the opentype font by modifying the respective font mapping in this file.

To work around the issue of mangled fonts, ArcSight recommends that you:

- 1 Install a localized Adobe Reader 8.0 depending on the language of your platform on your Manager machine. This version of the Adobe Reader installs the opentype fonts by default.
- 2 Edit the `server.properties` file as follows:
  - a Set `report.font.truetype.path` property to point to the directory that contains the truetype and opentype font. On Windows it is typically `C:\WINNT\fonts;C:\Program Files\Adobe\Reader 8.0\Resource\CIDFont` where ";" is used as a path separator to separate the multiple paths. Use ":" as a path separator in Unix. On Unix platforms, the truetype font path may differ depending on the specific Unix platform, but it is typically `/usr/lib/font`. The CIDFont directory is always the same relative to the Adobe Reader installed directory. So, the default directory would be `/usr/lib/font:<adobe_reader_dir>/Resource/CIDFont`.
  - b Set `report.font.cmap.path` property to point to Adobe Reader's CMap directory. On windows, it is typically `C:\Program Files\Adobe\Reader 8.0\Resource\CMap`. On Unix, the CMap path is relative to the Adobe Reader installation -- `<adobe_reader_dir>/Resource/CMap`.

## E-mail notification doesn't happen.

If you receive the following error:

```
[2009-12-03 14:31:33,890][WARN
][default.com.arcsight.notification.NotifierBase][send] Unable to
send out e-mail notification, notifications have not been
configured.
```

- Verify the following properties are set in the `server.properties` file:
 

```
notifications.enable=true
```

 and
 

```
notifications.incoming.enable=true
```
- Check `server.properties` file to find which SMTP server is associated with the Manager. Make sure that the SMTP server is up and running.
 

Review the Notification resource and confirm the e-mail address and other configuration settings.

## Notification always escalates.

Check `server.properties` file to find which POP3 or IMAP server is associated with the Manager. Make sure that the POP3 or IMAP server is up and running, in order to process acknowledgements from notification recipients.

## Pager notification doesn't happen.

Check `server.properties` file to find which SNPP server is associated with the Manager. Make sure that the SNPP server is up and running.

## Query or report performance degrades suddenly.

- Check that the ArcSight Database host has sufficient disk space.
- Check that the ArcSight Database statistics are up to date.
- Has the network infrastructure changed?
- Has the ArcSight Database or DBMS configuration changed?

See also, [“Query and Trend Performance Tuning” on page 158](#) for more information on performance enhancements and suggestions on how to improve performance with regard to queries and trends.

## Query and Trend Performance Tuning

Previous to ESM v.4.0 SP1, some trends exceeded 10 hours to execute queries. This eventually caused these queries to fail or lead to ESM scheduler problems. This effect was most pronounced on systems with high event rates (typically thousands of events per second).

To resolve this issue, various queries used by the trends in the default ArcSight system content were studied to ensure that the database was choosing optimal query execution plans. In a number of cases, the execution plan was not optimal and database "hints" were added to the queries to optimize the query execution. Most of these queries were sped up, some of them by a significant amount (much more than a factor of 10).

We have enhanced the scheduler to allocate two threads for processing system tasks. This change alleviates performance issues caused by conflicts between system tasks and user level tasks within the scheduler.

Starting in ESM v.4.0 SP1, Patch 3, several performance enhancements related to queries and trends were included. All follow-on service packs, patches, and releases include these performance enhancements, configurable properties, and reports. The following sections detail these, and also provide other troubleshooting tips.

## Regenerate Event Statistics

Regenerate event statistics using the following command if you are experiencing query performance issues. To regenerate event statistics, run this command in `ARCSIGHT_HOME\bin` on your database machine:

```
./arcdbutil sql username/password  
@../utilities/database/oracle/common/sql/  
RegenerateEventStats.sql
```

The `RegenerateEventStats.sql` command deletes statistics on event tables and indexes generated using the `ANALYZE` command, and regenerates the partition statistics using the `DBMS_STATS` command.



**Note**

The time that the `RegenerateEventStats.sql` command takes to complete depends on the number of events in your database and can take from several minutes to a few hours.

---

## Persistent Database Hints

Database hints are provided in system content packages. These hints are not visible in the Console. Please do not attempt to modify the system queries through the Console because this will cause the hint to disappear and the query will run slowly again.

### server.defaults.properties Entries for Trends

- `trends.query.timeout.seconds=7200`

This is the amount of time that a trend query is allowed to run, in seconds, before the SQL statement times out and the trend query fails. If absent or 0, no time-based timeout is applied.

- `trends.query.timeout.percent=50`

This is the amount of time that a trend query is allowed to run, as a percentage of the query interval for interval trends, before the SQL statement times out and the trend query fails. If absent or 0, no percentage-based timeout is applied.

As an example, with a 50 percent setting, a query covering a start/end time range of 1 hour will time out after 30 minutes. A start/end time range covering 1 day would time out after 12 hours.

If both timeouts are specified, the system will use the smaller of the two.

- `trends.query.failures.deactivation.threshold=3`

If this many consecutive "accumulate" (not refresh) runs fail for any reason, the system automatically disables the trend. The check is always performed after any accumulate query run fails. Once the threshold is reached, any remaining queries to be executed by this task are skipped. If this setting is absent or 0, the checking mechanism is turned off.

If a trend or query is stopped because of any of the above reasons, an audit event will reflect this.

## Troubleshooting Checklist after Restarting the Manager

- Use the Console Trend Editor to manually disable any trends that you do not need or that you notice have excessive query times. Disabling these trends will help reduce scheduler and database contention.
- Your own custom trends may have long-running queries and may be timing out. If this is the case, use the Query Tuner tool provided with this patch. See the description on querytuner in the ArcSight Commands appendix for instructions on how to use this tool. Once you have identified a hint that might help, please contact ArcSight support and provide a package with your query or queries for ArcSight to examine. We will investigate and determine if database hints can improve your trend queries.
- As trend data gathering tasks wake up, the trend will attempt to fill in the gaps for missing intervals. Depending on the size of the gaps, this may take some time before the trends catch up.
- A trend will not usually re-run any previously failed runs. If you want to re-run a particular time, you need to manually request it from the Trend Editor.

## Reports for Monitoring Trend Performance

The following new reports are available as a part of this Patch. We recommend running these reports after installing the Patch to monitor the trend performance:

```
/All Reports/ArcSight Administration/Resource  
Monitoring/Trends/Trend Query Runs Duration
```

```
/All Reports/ArcSight Administration/Resource  
Monitoring/Trends/Skipped Scheduled Tasks
```

## Disable these Trends on High Throughput Systems

If your system environment typically processes a very large number of events per second (EPS) (e.g., over 1000 EPS or 100 million events per day), we recommend that you manually disable the following 9 trends, which are enabled by default:

```
/All Trends/ArcSight Administration/User/ArcSight User Login Trends  
- Hourly
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/Asset  
Configuration Change Tracking/Host Configuration Modifications
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/Asset  
Restarts/Asset Startup and Shutdown Events - Daily Trend
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/User  
Account Modifications/User Account Creation
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/User  
Account Modifications/User Account Modifications
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Reconnaissance/Port Scanning
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Reconnaissance/Zone Scanning Events by Priority
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Vulnerability View/Prioritized Vulnerability Events by  
Zone
```

```
/All Trends/ArcSight Foundation/Network Monitoring/Overall Traffic
```

## How will you know when a trend is caught up?

You can use either of the following techniques, both using the ESM Console UI:

- Using the Trend Data Viewer from within the Trends resource tree, you can see at most 2000 rows of data. (Select a trend in the resource tree, right-click, and choose **Data Viewer**.) Sort the trend timestamp column so that the timestamps show newest to oldest and observe when the newest value indicates it has caught up.
- Using the **Refresh...** button in the Trend Editor, set the start time as far back as needed (days or weeks) to see any entries and click Refresh to see which runs show up as available to be refreshed. Only the most recent ones should show first. Note that you should not actually refresh any runs, but only use this technique to see what has been run.

## How long will it take a trend to catch up?

This depends on how long the underlying query interval is, but a trend will typically do up to 48 runs, as needed, when it wakes up.



For a trend that queries an entire day and runs once a day, this would allow for more than a month's worth of data to be queried. The data must be present on the system, however, or the query will return no results (but it will not fail).

## Enhancing the Performance Globally for all Database Queries

You can enhance the performance for all queries made against the database. When Oracle Optimizer decides on a query execution plan, it can dynamically do a sampling of actual data to estimate the cost of the query. Based on the findings of this sampling, the Optimizer comes up with the best query execution plan which will help improve query performance. To enable dynamic sampling, run:

```
% arcdbutil sql
```

```
Enter user-name: / as sysdba
```

```
SQL> @<ARCSIGHT_HOME>\utilities\database\oracle\common\sql\
```

```
SetDynamicSampling.sql
```

In addition to Dynamic Sampling, you can update the IO transfer speed in the database which will help in query performance. If you do not update the IO transfer speed, Oracle defaults to a very low IO transfer speed estimate that adversely affects the query execution plan. Run the following command (while logged in as `sysdba`):

```
SQL> @ARCSIGHT_HOME\utilities\database\oracle\common\sql\
```

```
GatherSystemStats.sql
```

This script should also be run every time you make any storage hardware changes that affects IO transfer speeds.

## SmartConnectors

### My device is not one of the listed SmartConnectors.

ArcSight offers an optional feature called the FlexConnector Development Kit which may enable you to create a custom SmartConnector for your device.

ArcSight can create a custom SmartConnector. Contact ArcSight Customer Support.

### My device is on the list of supported products, but it does not appear in the SmartConnector Configuration Wizard.

Your device is likely served by a Syslog sub-connector of either file, pipe, or daemon type.

### Device events are not handled as expected.

Check the SmartConnector configuration to make sure that the event filtering and aggregation setup is appropriate for your needs.

### SmartConnector not reporting all events.

Check that event filtering and aggregation setup is appropriate for your needs.

## Some Event fields are not showing up in the Console.

Check that the SmartConnector's Turbo Mode and the Turbo Mode of the Manager for the specific SmartConnector resource are compatible. If the Manager is set for a faster Turbo Mode than the SmartConnector, some event details will be lost.

## SmartConnector not reporting events.

Check the SmartConnector log for errors. If the SmartConnector cannot communicate with the Manager, it will cache events until its cache is full.

## Partition Archiver problems.

See Partition Archiver under ["Database" on page 166](#).

## Console

### Can't log in with any Console.

Check that the ArcSight Manager is up and running. If the Manager is not obviously running, open a command window on `<ARCSIGHT_HOME>/bin`, and run:

```
./arcsight manager
```

If the Manager is running, but you still can't log in, suspect any recent network changes, such as the installation of a firewall that will affect communication with the Manager host.

### Can't log in with a specific Console.

If you can log in from some Console machines but not others, focus on any recent network changes and any configuration changes on the Console host in question.

### Console reports out of memory.

This can happen when you open many independent viewing channels. If you need to do this often, change the memory settings in the `console.bat` or `console.sh` file. Find the line that starts set `ARCSIGHT_JVM_OPTIONS=` and change the parameter `-Xmx128m` to `-Xmx256m`. You must restart the Console for the new setting to take effect.

### Acknowledgement button is not enabled.

The Acknowledgement button is enabled when there are notifications to be acknowledged and they are associated with a destination that refers to the current user. To enable the button, add the current user to the notification destination.

### The grid view of Live security events is not visible.

To restore the standard grid view of current security events, select **Active Channels** from the Navigator drop-down menu. Double-click **Live**, found at `/Active channels/Shared/All Active channels/ArcSight System/Core/Live`

### The Navigator panel is not visible.

Press **Ctrl+1** to force the Navigator panel to appear.

## The Viewer panel is not visible.

Press **Ctrl+2** to force the Viewer panel to appear.

## The Inspect/Edit panel is not visible.

Press **Ctrl+3** to force the Inspect/Edit panel to appear.

## Internal ArcSight events appear.

Internal ArcSight events appear to warn users of situations such as low disk space for the ArcSight Database. If you are not sure how to respond to a warning message, contact ArcSight Customer Support.

## The Manager Status Monitor reports an error.

The Console monitors the health of the ArcSight Manager and the ArcSight Database. If a warning or an error occurs, the Console may present sufficient detail for you to solve the problem. If not, report the specific message to ArcSight Customer Support.

## Console logs out by itself.

Check the Console log file for any errors. Log in to the Console. If the Console logs out again, report the error to ArcSight Customer Support.

## Console stops responding when sending a test SNPP notification.

If the Console stops responding when sending a test SNPP notification, it may indicate that the SNPP port is blocked by a firewall or packet filtering device.

## Cannot log in to ArcSight Web from within the Console.

In ArcSight Console, if you click **File->Launch ArcSight Web**, it will start the browser within the Console window and display the ArcSight Web login screen. Once you enter your username and password for the Manager, you should be able to log into the Web from within the Console. However, if inspite of entering the correct login information, you cannot login to ArcSight Web and your browser appears to hang, then you have to change the security settings on your browser. To do so on Internet Explorer:

- 1** Go to **Tools->Internet Options**.
- 2** Click the **Security** tab.
- 3** Click the **Internet** icon.
- 4** Click the **Custom level...** button.
- 5** Select **Medium** from the **Reset to** drop down menu.
- 6** Click **Reset** button. You will receive a warning asking you whether you want to change the security setting of the zone. Click **Yes**.
- 7** Click **OK** in the Security Options box.
- 8** Click **OK** in the Internet Options box.

- 9 Go back to the Console and try to restart ArcSight Web from within the Console by clicking **File->Launch ArcSight Web**.

## Console does not start in Windows 2008

If you installed and then started the Console in Windows 2008, you may get an error due to access refusal. In Windows 2008, make sure to configure the User Access Control (UAC) of the ESM Console user. Consult the Microsoft website for more details on UAC specific to Windows 2008.

## Manager

### Can't start Manager.

The ArcSight Manager will provide information on the command console which may suggest a solution to the problem. Additional information will be written to `<ARCSIGHT_HOME>/logs/default/server.std.log`.

To check database connectivity manually, open a command window on `<ARCSIGHT_HOME>/bin` (on the Manager host) and run:

```
arcsight testdbconnection
```

### Manager shuts down.

The Manager stops when it encounters a fatal error. The file `<ARCSIGHT_HOME>/logs/default/server.std.log` will have more details about the error condition.

For example, the following error indicates that a connection cannot be established with the underlying Oracle DBMS:

```
[ERROR][default.com.arcsight.common.persist.oracle.OracleDatabaseI
nfoBroker][getDatabaseInfo]

com.arcsight.common.persist.PersistenceException: Unable to get
connection: Io exception: Connection reset by peer: socket write
error
```

This indicates that the Oracle TNS Listener is running but the actual ArcSight Database service is not reachable.

### Manager restarts automatically.

If the Java Virtual Machine (JVM) fails to respond within two minutes, an ArcSight watchdog program will automatically restart it, which reduces system performance but does not cause data loss. This situation has been observed on low-end Windows-based host machines with pagefile size optimization enabled. Optimization complicates the garbage collection process, rendering the JVM non-responsive for longer than two minutes.

Disable pagefile size optimization. Perform the following steps to disable pagefile size optimization on Windows 2000 Manager hosts:

- 1 Right-click **My Computer** and select **Properties** from the menu. Select the **Advanced** tab.
- 2 Click **Performance Options** for Windows 2000.

- 3 Set **Initial size** to the same value as **Maximum size**.
- 4 Click **Set**.
- 5 Click **OK**.

## The log contains a warning “Side table for [name] is 100% full. System performance will be affected.”

This log error message is the result of the default sizes for side object caches being too small for some larger production deployments. Although system performance is generally not affected, to stop generating the warning message, add the following lines to the `server.properties` file and restart the ArcSight Manager:

```
persist.securityevent.stcache.GeoDescriptor=50000
persist.securityevent.stcache.AgentDescriptor=500
persist.securityevent.stcache.DeviceDescriptor=50000
persist.securityevent.stcache.CategoryDescriptor=3000
persist.securityevent.stcache.LabelsDescriptor=2000
persist.securityevent.stcache.ResourceRef=20000
```

If you continue to see the error message after this change, one or more SmartConnectors may be misconfigured. Contact ArcSight Customer Support.

## Scheduled Task Run is Off When Switching from Daylight Savings Time to Standard Time or Vice Versa.

- If the trigger time for a particular scheduled task run happens to fall during the transition time from DST to ST or vice versa, the interval for that particular run gets thrown off. The interval calculation for subsequent scheduled runs do not get affected.
- Currently, there are four time zones that are not supported in ESM:
  - ◆ Kwajalein
  - ◆ Pacific/Kwajalein
  - ◆ Pacific/Enderbury
  - ◆ Pacific/Kiritimati

These time zones fall in two countries, Marshall Islands and Kiribati.

## ArcSight Web

### Some content, particularly dashboards, is not visible.

Install the latest Adobe Flash plug-in to your browser. Visit the Adobe website to download this free plug-in.

### Can't log in to ArcSight Web.

Check that the ArcSight Web Server is up and running. If ArcSight Web is up, check that the ArcSight Manager is also up and running.

If the Manager is running, but you still can't log in, suspect any recent network changes, such as the installation of a firewall that will affect communication between the ArcSight Web server and the Manager host.

If you can log in to the ArcSight Console but not ArcSight Web, focus on any recent network changes and any configuration changes to your browser.

Make sure that the version number of ArcSight Web matches that of the Manager. If the version numbers do not match, log in will be disabled.

## Can't start ArcSight Web.

If the ArcSight Web Server cannot start, check that the ArcSight Manager is up and running. If the Manager is not obviously running, open a command window on `<ARCSIGHT_HOME>/bin`, and run:

```
./arcsight manager
```

Examine the ArcSight Web log file for specific error messages. If the message is not clear, contact ArcSight Customer Support.

## Database

### Partition Archiver can't connect to Manager.

Check the Partition Archiver log for errors. The log file is found in the logs directory:

```
<ARCSIGHT_HOME>/logs/default/agent.out.wrapper.log
```

An SSL Handshake exception in the log indicates a problem with the Manager's certificate. From the SmartConnector's install directory, run the following command to establish a valid certificate:

```
./arcsight agent tempca -ac
```

### Oracle hangs without warning.

If automatic archive log mode is turned on, Oracle will hang if the archive log destination becomes full. Oracle will resume when you make archive log space available.

### An e-mail notification reports a problem with the ArcSight Database.

Don't ignore a warning or error notification from the ArcSight system. If the message is not clear to you, contact ArcSight Customer Support. Ignoring a database error can lead to the Manager suddenly stopping, which will eventually lead to security event data loss.

See Appendix C, Monitoring Database Attributes, for more information.

### Partition logs may not be complete.

Only one duplicate log file can be written to at one time. Therefore, if a partition utility is in progress and another partition utility starts in parallel, the logs for the first utility will not be written anymore to the duplicate log file. However, the log data for the first utility is not lost; it is available in the `<ARCSIGHT_HOME>/logs/server.log` file.

See the “Database Administration” chapter, for more information.

## SSL

### Cannot connect to the SSL server: IO Exception in the server logs when connecting to the server

Causes:

The SSL server may not be running.

- A firewall may be preventing connections to the server.

Resolutions:

- Ensure that the SSL server is running.
- Also, ensure that a firewall is not blocking connections to the server.

### Cannot connect to the SSL server

The hostname to which the client initiates an SSL connection should exactly match the hostname specified in the server SSL certificate that the server sends to the client during the SSL handshake.

Causes:

- You may be specifying Fully Qualified Domain Name (FQDN) when only hostname is expected or the other way around.
- You may be specifying IP address when hostname is expected.

Resolutions:

- Type exactly what the server reports on startup in `server.std.log` (“Accepting connections at `http://...`”)
- For Network Address Translation (NAT) or multi-homed deployments, use hosts file to point client to correct IP.

### PKIX exchange failed/could not establish trust chain

Cause:

Issuer cannot be found in trust store, the cacerts file.

Resolution:

Import issuer's certificate (chain) into the trust store.

### Issuer certificate expired

Cause:

The certificate that the SSL server is presenting to the client has expired.

Resolution:

Import the latest issuer's certificate (chain) into the trust store.

## Cannot connect to the Manager: Exception in the server log

### Cause:

If you replaced the Manager's key store, it is likely that the old key store password does not match the new password.

### Resolution:

Make sure the password of the new key store matches the old key store. If you do not remember the current key store's password, run the Manager Configuration Wizard on the Manager (ArcSight Web Configuration Wizard on the Web) to set the password of the current key store to match the new key store's password.

## Certificate is invalid

### Cause:

The timestamp on the client machine might be out of the bounds of the validity range specified on the certificate.

### Resolution:

Make sure that the current time on the client machine is within the validity range on the certificate.

## Issue with Internet Explorer and ArcSight Web in FIPS Mode

When using Internet Explorer (IE) with ArcSight Web running in FIPS mode, IE may return an error message when you attempt to log in using username and password authentication:

- ArcSight Web is FIPS-enabled
- You have opted to use Password Based or SSL Client Based Authentication
- You use ActivClient middleware and have registered the certificate from Smart Card into Internet Explorer
- You have enabled TLS v1 on Internet Explorer
- ArcSight Web's truststore contains the Smart Card issuer's certificate
- The card is not present in the card reader

This is an issue with Internet Explorer. To use the password based authentication in FIPS 140-2 mode, you need to remove all registered PKCS#11 related certificates from the Internet Explorer certificate repository. To do so:

- 1 Go to **Tools->Internet Options** and click the **Content** tab.
- 2 Click **Certificates** and then select the **Personal** tab.
- 3 Select all the PKCS#11 related certificates and click **Remove**.
- 4 Click **Intermediate Certification Authorities**.
- 5 Select all the PKCS#11 related certificates and click **Remove**.



# Monitoring Database Attributes

---

This chapter provides information about in-built checks that monitor database attributes and generate warning or error messages, as appropriate.

This appendix is divided into the following sections:

[“Understanding Database Checks” on page 169](#)

[“Disabling Database Checks” on page 171](#)

[“List of Database Check Tasks” on page 171](#)

## Understanding Database Checks

ArcSight ESM provides in-built checks to monitor configurations and runtime attributes of your database. These checks inform you if attributes such as password of the Oracle account or number of available reserve partitions drop below an acceptable value. Depending on the severity of deviation, a warning or an error message is generated.

If an error or a warning message is generated, these actions take place:

- A message is logged to the `server.std.log` file on the Manager.
- If you have configured the Manager to generate an e-mail message, a message is sent.
- A notification message is displayed on the ArcSight Console.

If an error message is generated, the event flow to the Manager is stopped. In that case, SmartConnectors start caching the events so there is no loss of events. After you have resolved the issue that caused the error, you can click a reactivation URL that is included in the error message to restart the event flow.

Each check task is scheduled to run at a predefined interval and compare the current system state with a predefined threshold, both of which can be changed to suit your needs.

The interval and threshold for each task is defined in the `server.defaults.properties` file on the Manager. You can override these values in the `server.properties` file on the Manager.

## Message text

The following is an example of the error or warning e-mail message that is sent:

Date: Fri, 14 Apr 2006 01:24:36 +0000 (GMT+00:00)

To: administrator@mycompany.com

```
[-- Attachment #1 --]

[-- Type: text/plain, Encoding: 7bit, Size: 1.0K --]

== SUBSYSTEM STATUS CHANGED
=====

Error - Event Receiver

== ORIGIN OF CHANGE
=====

Error - PartitionManagerCheckTaskTracker

-- DESCRIPTION -----
-----

[PartitionManagerCheckTaskTracker: Fatal Error: There are only 0
of 7 reserve

partitions available. This is likely due to failures in Partition
Manager

runs for the past few days. If this situation is not fixed, the MAX
partition

will become the CURRENT partition in the next few days, causing
system failure.

Check the Partition Manager logs for errors and fix the problem
before

proceeding.

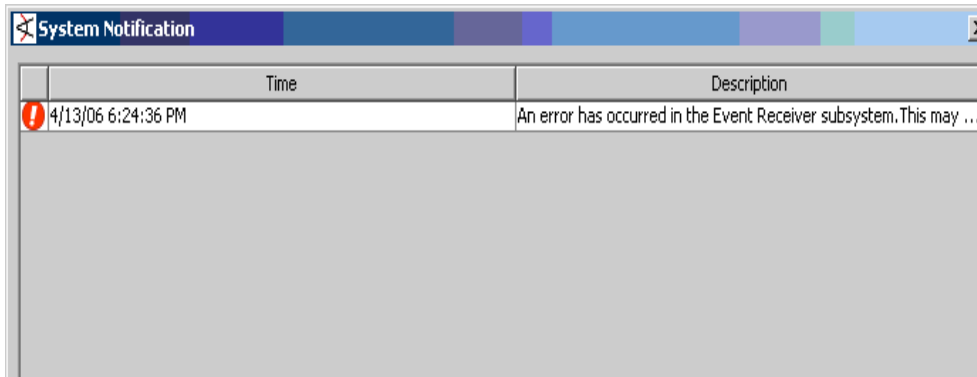
Fix the root cause of the error reported. If the event flow is
stopped, use the

following URL to resume:

https://yourmanager.mycompany.com:8443/arcsight/web/reactivate.jsp
?id=87160D7E0425A22FBE5354FE90387A96

]
```

The following is an example of the notification message that is displayed on the Console:



Time	Description
4/13/06 6:24:36 PM	An error has occurred in the Event Receiver subsystem. This may ...

## Disabling Database Checks

If you do not want to run a specific database check, you can disable it.

To disable a database check task, specify the name of the check task as the value for the `whine.check.exclude` property in the `server.properties` file on the Manager.



To obtain the name of a task, see List of Database Check Tasks.

For example, to exclude `PartitionManagerCheckTask`, enter this in the `server.properties` file:

```
whine.check.exclude=PartitionManagerCheckTask
```

To exclude multiple check tasks, specify a comma-separated list for the `whine.check.exclude` property; for example,

```
whine.check.exclude=PartitionManagerCheckTask,
PartitionCompressorCheckTask
```

## List of Database Check Tasks

The following is a list of check tasks available in this ArcSight ESM release. Each check task includes an interval at which that task is performed, any attributes that are checked, and the default thresholds at which a Warning or Error message is generated.

### 1 AccountCheckTask - Checks User Account Expiry

```
# AccountCheckTask is run every 12 hours
whine.check.interval.AccountCheckTask=43200

# AccountCheck Password Expiry warning threshold (days)
dbcheck.oracle.account.warn.threshold=5

# AccountCheck Password Expiry error threshold (days)
dbcheck.oracle.account.error.threshold=2
```

### 2 ArchiveDestinationCheckTask - If the redo log archive destination is cross mounted in the manager box, this task will check for space availability in such a destination

```
# ArchiveDestinationCheckTask is run every 1 hour
whine.check.interval.ArchiveDestinationCheckTask=3600

# Whether database archive destination filesystems are cross mounted in the Manager
box
dbcheck.oracle.archivedest.xmount=false

# Minimum number of hours of archive space that should be available
dbcheck.oracle.archivedest.threshold.hours=18
```

- 3 ArchiveSessionCheckTask** - Checks whether any Oracle sessions are stuck on "archive required" wait event.

```
# ArchiveSessionCheckTask is run every 30 seconds
whine.check.interval.ArchiveSessionCheckTask=30
```

- 4 ParameterCheckTask** - Checks default and non-default Oracle parameters against values specified below.

```
# ParameterCheckTask is run every 24 hours
whine.check.interval.ParameterCheckTask=86400

# Suggested % of shared_pool in terms of total sga
dbcheck.oracle.parameter.sharedpool=20

# Suggested % of db_cache in terms of total sga
dbcheck.oracle.parameter.dbcache=40

# Suggested minimum db_files value
dbcheck.oracle.parameter.dbfiles=200

# Suggested maximum java_pool size
dbcheck.oracle.parameter.javapool=0

# Suggested minimum log_buffer size
dbcheck.oracle.parameter.logbuffer=1048576

# Suggested maximum parallel_max_servers value
dbcheck.oracle.parameter.parallelmaxservers=0

# Suggested pga_aggregate_target value
dbcheck.oracle.parameter.pgaaggreatarget=40

# Suggested minimum processes value
dbcheck.oracle.parameter.processes=100

# Suggested minimum undo_retention value
dbcheck.oracle.parameter.undoretention=43200

# Suggested timed_statistics value
dbcheck.oracle.parameter.timedstatistics=TRUE

# Suggested workarea_size_policy value
dbcheck.oracle.parameter.workareasizepolicy=AUTO
```

- 5 PartitionArchiverCheckTask** - Checks whether partition archiver is working successfully.

```
# PartitionArchiverCheckTask is run every 12 hours
whine.check.interval.PartitionArchiverCheckTask=43200

# Archiver Lag Warning Threshold
dbcheck.oracle.archiver.warnthreshold=2
```

- 6 PartitionCompressorCheckTask** - Checks whether partition compressor is working successfully.

# PartitionCompressorCheckTask is run every 12 hours

`whine.check.interval.PartitionCompressorCheckTask=43200`

- 7 PartitionManagerCheckTask** - Checks whether enough reserve partitions are available.

# PartitionManagerCheckTask is run every 12 hours

`whine.check.interval.PartitionManagerCheckTask=43200`

# Partition Manager Warning Threshold (# of available reserve partitions)

`dbcheck.oracle.manager.warnthreshold=5`

# Partition Manager Error Threshold (# of available reserve partitions)

`dbcheck.oracle.manager.errorthreshold=2`



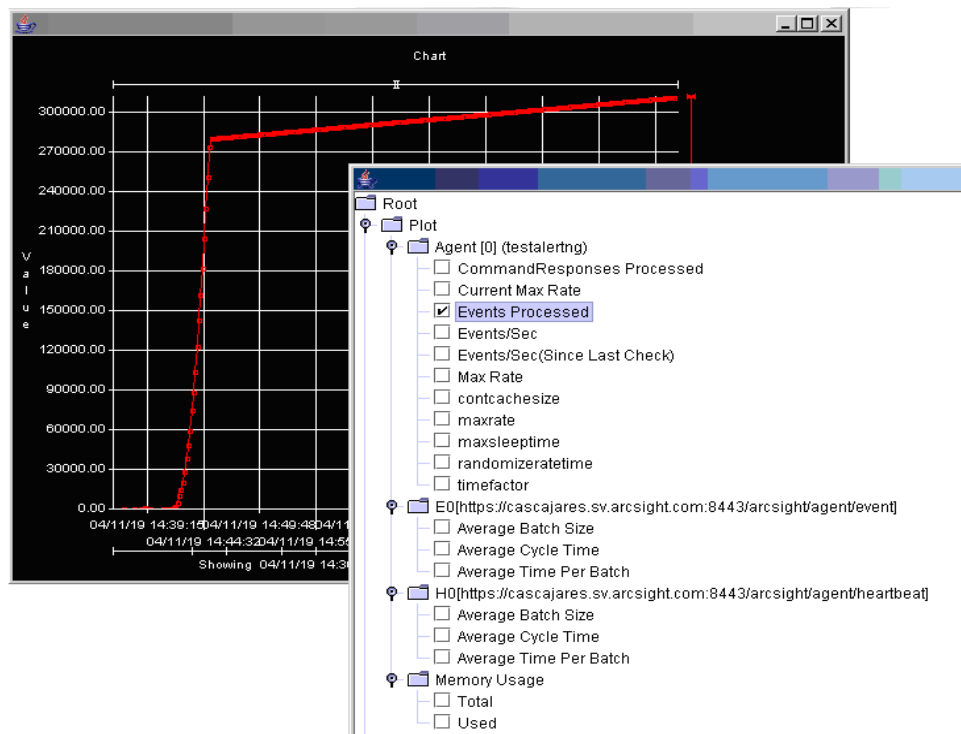
## Appendix D

# The Logfu Utility

This appendix is divided into the following sections:

- “Running Logfu” on page 176
- “Example” on page 178
- “Troubleshooting” on page 178
- “Menu” on page 180
- “Typical Data Attributes” on page 180
- “Intervals” on page 181

Logfu is an ArcSight utility that analyzes log files. It is indispensable for troubleshooting problems that would otherwise require poring over text logs. Logfu generates an HTML report ([logfu.html](#)) and, especially in SmartConnector mode, includes a powerful graphic view of time-based log data. Logfu pinpoints the time of the problem and often the cause as well.



**Figure D-1** Logfu has two windows: the interactive Chart and the Plot/Event window.

## Running Logfu

Logfu finds log files in the current directory. The `-a` or `-m` or `-c` switches tell it which file names to look for. The `-m` switch tells it to look for all three Manager logs—`server.std.log`, `server.log`, and `server.status.log`—for example.

To run Logfu, follow these steps:

- 1 Open a command or shell window in `<ARCSIGHT_HOME>/logs/default`. This refers to the logs directory under the ArcSight installation directory. (Path separators are `/` for Unix and `\` for Windows.) Logfu requires an X Windows server on Unix platforms.
- 2 Run logfu for the type of log you will analyze:  
  
For Manager logs, run: `../bin/arcsight logfu -m`  
  
For SmartConnector logs, run: `../bin/arcsight agent logfu -a`
- 3 Right-click in the grid and select **Show Plot/Event Window** from the context menu.
- 4 Check at least one attribute (such as Events Processed) to be displayed.

The initial display is always an empty grid. Loading very large log files can take a few minutes (a 100MB log might take 5 or 10 minutes). Once log files are scanned, the information gleaned from them is cached (in files named `data.*`) that will speed up loading the second time. If something about the log changes, however, you must manually delete the cache files to force logfu to reprocess the log.

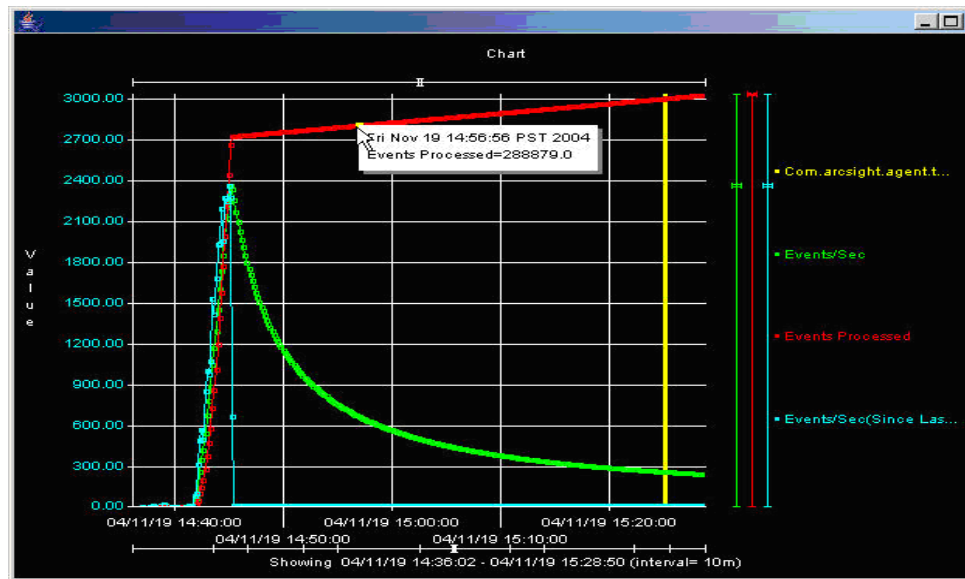
Right-click the grid and choose **Show Plot/Event Window** from the context menu. Select what to show on the grid from the **Plot/Event Window** that appears.

The tree of possible things to display is divided into Plot—attributes that can be plotted over time, like events per second—and Event—one-time things, like exceptions, which are shown as vertical lines. Check as many things as you want to show.

Because SmartConnectors can talk to multiple Managers and each can be configured to use multiple threads for events, the Plot hierarchy includes nodes for each SmartConnector and each Manager. Within the SmartConnector, threads are named `E0`, `E1`, and so on. Each SmartConnector has one heartbeat thread (`H0`) as well. Different types of SmartConnector



(firewall log SmartConnector, IDS SNMP SmartConnector, and so on) have different attributes to be plotted.



**Figure D-2** The interactive Chart uses sliders to change the view. Hovering over a data point displays detailed information.

There are two horizontal sliders—one at the top of the grid, one underneath. The slider at the top indicates the time scale. Drag it to the right to zoom in, or widen the distance between time intervals (vertical lines). The slider at the bottom changes the interval between lines—anywhere from 1 second at the far left to 1 day at the far right. The time shown in the grid is listed below the bottom slider:

Showing YY/MM/DD HH:MM:SS - YY/MM/DD HH:MM:SS (Interval= X)

Click anywhere in the grid area and drag a green rectangle to zoom in, changing both the vertical and horizontal scales at once. Hold the **Ctrl** key as you drag to pan the window in the vertical or horizontal direction, and hold both the **Shift** and **Ctrl** keys as you drag to constrain the pan to either vertical or horizontal movement. When you are panning, only sampled data is shown, but when you stop moving, the complete data will fill in. (You can change this by unchecking **Enable reduced data point rendering** in Preferences.)

Hover the mouse over a data point to see detailed information in a “tooltip” window, as shown in [Figure D-2](#).

For each attribute being plotted, a colored, vertical slider appears on the right of the grid. This slider adjusts the vertical (value) scale of the thing being plotted.

By default, data points are connected by lines. When data is missing, these lines can be misleading. To turn off lines, uncheck **Connect dots** in Preferences.

Once you have specified attributes of interest, scaled the values, centered and zoomed the display to show exactly the information of concern, select **Save as JPG** on the menu to create a snapshot of the grid display that you can print or e-mail. The size of the output image is the same as the grid window, so maximize the window to create a highly detailed snapshot, or reduce the window size to create a thumbnail.

## Example

Perhaps a particular SmartConnector starts by sending 10 events per second (EPS) to the Manager, but soon is sending 100, then 500, then 1000 EPS before dropping back down to 10. Logfu lets you plot the SmartConnector's EPS over time—the result is something like a mountain peak.

When you plot the Manager's receipt of these events, you might see that it keeps up with the SmartConnector until 450 EPS or so. You notice that the Manager continues consuming 450 EPS even as the SmartConnector's EPS falls off. This is because the Manager is consuming events that were automatically cached.

By plotting the estimated cache size, you can see the whole story—the SmartConnector experienced a peak event volume and the cache stepped in to make sure that the Manager didn't lose events, even when it couldn't physically keep up with the SmartConnector.

Use the vertical sliders on the right to give each attribute a different scale to keep the peak EPS from the SmartConnector from obscuring the plot of the Manager's EPS.

## Troubleshooting

Another real-world example involved a Check Point SmartConnector that was mysteriously down for almost seven days. Logfu plotted the event stream from the SmartConnector and it was clearly flat during the seven days, pinpointing the outage as well as the time that the event flow resumed. By overlaying Check Point Log Rotation events on the grid, it became clear that the event outage started with a Log Rotation and that event flow resumed coincident with a Log Rotation.

Further investigation revealed what had happened—the first Check Point Log Rotation failed due to lack of disk space, which shut down event flow from the device. When the disk space problem had been resolved, the customer completed the Log Rotation and event flow resumed.

If the Manager suddenly stops seeing events from a SmartConnector Logfu helps determine whether the SmartConnector is getting events from the device. Another common complaint is that not all events are getting through. Logfu has a plot attribute called 'ZFilter'—zone filter—that indicates how many raw device events are being filtered by

the SmartConnector. Events processed (the number of events sent by the device) minus ZFilter should equal Sent (the number of events sent to the Manager).

Logfu

Analizers

Name	agent.log	Path	null/	Elapsed	0 mins 2 secs 203 ms
				Total	0 mins 2 secs 203 ms

Sessions by Length

[1]	00:00:48:16:869	[0]	00:00:04:24:631
-----	-----------------	-----	-----------------

Sessions by Throughput

[0]	0.0	[1]	0.0
-----	-----	-----	-----

Sessions by Exception count

[0]	0	[1]	0
-----	---	-----	---

Sessions by longest Full GC

All Sessions

[0]	[1]
-----	-----

Session 0

Start	04-11-19 14:35:17	ArcSightBuildVersionInfo	r_11-8-200_20:17:33
End	04-11-19 14:39:41	ArcSightSystemVersion	3.0.1.0.0
Length	0 days 0 hrs 4 mins 24 secs	Event Transport [0]	https://ca:8443/arcsight/agent/event
log filename	agent.log	Heartbeat Transport [0]	https://ca:8443/arcsight/agent/heartbeat
Throughput	0.0		
Avg Insert Threads	0.0		

**Figure D-3** The HTML report for the log file shown in Figure 1.

## Menu

Menu Item	Description
<b>Show Plot/Event Window</b>	Presents the possible attributes to be displayed
<b>Bring To Front</b>	
<b>Send to Back</b>	
<b>Undo Zoom</b>	Return to previous view
<b>Zoom out</b>	
<b>Auto Scale</b>	Fit all data on the grid
<b>Save as JPG</b>	Save a snapshot of the current view on the grid
<b>Go to</b>	Display the line of the log file which corresponds to a particular data point
<b>Reset</b>	Clear all checked attributes and restore the normal startup view of an empty grid
<b>Preferences</b>	Check:  Connect dots – draw lines between data points  Enable fast rendering  Enable reduced data point rendering

---

## Typical Data Attributes

SmartConnector Specific

Menu Item	Description
CommandResponses Processed	Number of Get Status calls from the Manager
Current Max Rate	
Events Processed	
Events/Sec	Averaged events per second
Events/Sec (Since Last Check)	Events per second in last minute (unless check time is configured to a different interval)
Max Rate	
contcachesize	Contiguous Cache Size
maxrate	Maximum Rate
maxsleeptime	Maximum Sleep Time
randomizeratetime	Randomize Rate Time
timefactor	

## For Each SmartConnector Thread

Menu Item	Description
Average Batch Size	Number of events per batch (typically ~ 100)
Average Cycle Time	Duration of transport and Manager acknowledgement
Average Time Per Batch	Should be under 1 minute

## Memory Usage

Menu Item	Description
Total	Total available memory
Used	Memory used

## Events

Menu Item	Description
SmartConnectors Initializing	SmartConnector startup
com.arcsight.agent.transport.TransportException	
com.arcsight.common.agent.ServerConnectionException	
java.net.SocketException	
Forcing disconnection	Transport event—Manager disconnecting.

## Intervals

1 second

5 seconds

10 seconds

30 seconds

1 minute

5 minutes

10 minutes

30 minutes

1 hour

6 hours

12 hours

1 day

# Appendix E

## Creating Custom E-mails Using Velocity Templates

---

This appendix describes how to modify Velocity templates to customize e-mail messages you receive from the ArcSight notification system.

This appendix is divided into the following sections:

[“Overview” on page 183](#)

[“Notification Velocity templates” on page 183](#)

A sample use case is presented to illustrate the concept.

### Overview

ArcSight supports the use of Velocity templates that are a means of specifying dynamic input to the underlying Java code.

You can apply Velocity templates in a number of places in ArcSight. For a complete list of Velocity template applications in ArcSight, see the Console online Help.

This section describes one such application—E-mail Notification Messages—in detail. You can use Velocity templates on your Manager to create custom e-mail messages to suit your needs.

### Notification Velocity templates

The `<ARCSIGHT_HOME>/Manager/config/notifications` directory contains the following two Velocity templates for customizing e-mail notifications:

- `Email.vm`—The primary template file that calls secondary template files.
- `Informative.vm`—The default secondary template file.

### Commonly used elements in Email.vm and Informative.vm files

It is important to understand the commonly used Velocity programming elements in the `Email.vm` and `Informative.vm` files before editing these files.

#### The #if statement

The general format of the #if statement for string comparison is:

```
#if ($introspector.getDisplayValue($event, ArcSight_Meta_Tag)
Comparative_Operator Compared_Value)
```

The #if statement for integer comparison is:

```
#if ($introspector.getValue($event,
ArcSight_Meta_Tag).intValue()Comparative_Operator Compared_Value)
```

You can specify `ArcSight_Meta_Tag`, `Comparative_Operator`, and `Compared_Value` to suit your needs.

`ArcSight_Meta_Tag` is a string when using the #if statement for string comparison (for example, `displayProduct`) and is an integer for the #if statement for integer comparison (for example, `severity`).

For a complete listing of ArcSight meta tags, see the Token Mappings topic in ArcSight FlexConnector Guide.

`Comparative_Operator` is `==` for string comparison; `=`, `>`, and `<` for integer comparison.

`Compared_Value` is a string or an integer. For string comparison, enclose the value in double quotes (" ").

## Contents of Email.vm and Informative.vm

The default `Email.vm` template file contents are:

```
## This is a velocity macro file...

## The following fields are defined in the velocity macro.

## event == the event which needs to be sent.

## EVENT_URL == root of the event alert.

## NOTIFICATION_URL == URL of the notifications page in ArcSight
Web

#parse ("Informative.vm")
```

This message can be acknowledged in any of the following ways:

- 1) Reply to this email. Make sure that the notification ID listed in this message is present in your reply)
- 2) Login to the ArcSight Console and click on the notification button on the status bar
- 3) Login to ArcSight Web at \${NOTIFICATION\_URL}

To view the full alert please go to at \${EVENT\_URL}

The default `Informative.vm` template file contents are:

```
=== Event Details ===

#foreach( $field in $introspector.fields )

#if( $introspector.getDisplayValue($event, $field).length() > 0 )
```



```

${field.fieldDisplayName}: $introspector.getDisplayValue($event,
$field)

#end

#end

```

## How the Email.vm and Informative.vm Template Files Work

Email.vm calls the secondary template file Informative.vm (#parse ("Informative.vm")). The Informative.vm file lists all the non-empty fields of an event in the format fieldName : fieldValue.

## Understanding the Customization Process

If you want to customize the template files to suit your needs, ArcSight recommends that you create new secondary templates containing fields that provide information you want to see in an e-mail for a specific condition.

For example, if you want to see complete details for an event—Threat Details, Source Details, Target Details, and any other information—generated by all Snort devices in your network, create a secondary template file called Snort.vm in <ARCSIGHT\_HOME>/config/notification, on your Manager, with the following lines:

```

=== Complete Event Details ===

Threat Details

Event: $introspector.getDisplayValue($event,"name")

Description:
$introspector.getDisplayValue($event,"message")

Severity:
$introspector.getDisplayValue($event,"severity")

-----
--

Source Details

Source Address:
$introspector.getDisplayValue($event,"attackerAddress")

Source Host Name:
$introspector.getDisplayValue($event,"attackerHostName")

Source Port:
$introspector.getDisplayValue($event,"sourcePort")

Source User Name:
$introspector.getDisplayValue($event,"sourceUserName")

-----
--

Target Details

```

```
Target Address:
$introspector.getDisplayValue($event,"targetAddress")

Target Host Name:
$introspector.getDisplayValue($event,"targetHostName")

Target Port: $introspector.getDisplayValue($event,"targetPort")

Target User Name:
$introspector.getDisplayValue($event,"targetUserName")

-----
--

Extra Information (where applicable)

Transport Protocol:
$introspector.getDisplayValue($event,"transportProtocol")

Base Event Count:
$introspector.getDisplayValue($event,"baseEventCount")

Template:
/home/arcsight/arcsight/Manager/config/notifications/Infosec.vm

-----
--
```

Once you have created the secondary templates, you can edit the `Email.vm` template to insert conditions that will call those templates.

As shown in the example below, insert a condition to call `Snort.vm` if the `deviceProduct` in the generated event matches "Snort".

```
#if( $introspector.getDisplayValue($event, "deviceProduct") ==
"Snort" )

#parse( "Snort.vm" )

#else

#parse( "Informative.vm" )

#end
```

## Customizing the template files

Follow these steps to customize the `Email.vm` and create any other secondary template files to receive customized e-mail notifications:

- 1 In `<ARCSIGHT_HOME>/config/notifications`, create a new secondary template file, as shown in the `Snort.vm` example in the previous section.
- 2 Save the file.
- 3 Edit `Email.vm` to insert the conditions, as shown in the example in the previous section.
- 4 Save `Email.vm`.

## Sample Output

If you use the `Snort.vm` template and modify `Email.vm` as explained in the previous section, here is the output these templates will generate:

```
Notification ID: fInjoQwBABCGMJkA-a8Z-Q== Escalation Level: 1

=== Complete Event Details ===

Threat Details

Event:                      Internal to External Port Scanning
Description:                Internal to External Port Scanning Activity
Detected; Investigate Business Need for Activity

Severity:                   2

-----
--

Source Details

Source Address:             10.129.26.37
Source Host Name:
Source Port:                0
Source User Name:          jdoe

-----
--

Target Details

Target Address:             161.58.201.13
Target Host Name:
Target Port:                20090
Target User Name:

-----
--

Extra Information (where applicable)

Transport Protocol:        TCP
Base Event Count:         1

Template:
/home/arcsight/arcsight/Manager/config/notifications/Snort.vm

-----
--

How to Respond

This message can be acknowledged in any of the following ways:
```

- 1) Reply to this email. Make sure that the notification ID listed in this message is present in your reply)
- 2) Login to the ArcSight Console and click on the notification button on the status bar
- 3) Login to myArcSight and go to the My Notifications Acknowledgment page at <https://mymanager.mycompany.com:9443/arcsight/app?service=page/NotifyHome>

To view the full alert please go to

<https://mymanager.mycompany.com:9443/arcsight/app?service=external/EventInspector&sp=SfInjoQwBABCGMJkA-a8Z-Q%3D%3D&sp=F&sp=F>

# The Archive Command Tool

---

This appendix is divided into the following sections:

[“Overview of the Archive Command Tool” on page 189](#)

[“Exporting Resources to an Archive” on page 190](#)

[“Importing Resources from an Archive” on page 191](#)

[“Syntax for Performing Common Archive Tasks” on page 194](#)



**Note**

You can use the packages feature to archive resources from and import resource to your ArcSight Database. For more information about packages and how to use them, see the Managing Packages topic in ArcSight Console Online Help. For information about the packages command, see Appendix A of this guide.

You can use the `archive` command line tool to import and export resource information stored in the ArcSight Database. You can use this tool in managing configuration information, for example, importing asset information collected from throughout your enterprise. You can also use this tool to archive resource information stored in the ArcSight Database so that, for example, prior to installing new versions of ESM, you can simply restore all the resource information after completing the installation.

When archiving information from the ArcSight Database, the `archive` command automatically creates the archive files you specify, saving resource objects in XML format. This documentation does not provide details on the structure of archive files and the XML schema used to store resource objects for re-import into ESM. If you have any special requirements for importing and exporting archive files, please contact your ArcSight representative.

## Overview of the Archive Command Tool

The ArcSight `archive` command tool can be run in two basic modes, remote or standalone. In remote mode, you can perform resource import or export operations from either an ArcSight Manager or ArcSight Console installation and can perform archive operations while ArcSight Manager is running. In standalone mode, from the computer where ArcSight Manager is installed, you can connect directly to the ArcSight database to

import or export resource information, however, ArcSight Manager must be shut down before you perform archive operations.

**Caution**

Do not run the archive tool in standalone mode against a database currently in use by an ArcSight Manager as it is possible to corrupt the database.

The basic syntax for the `archive` command is the following:

Remote `archive` Command Syntax:

```
arcsight archive -u Username -m Manager [-p Password] -f Filename  
[-i | -sort] [-q] ...
```

**Caution**

The cacerts file on the Manager host must trust the Manager's certificate. You may have to update cacerts if you are using demo certificates by running:

```
arcsight tempca -ac
```

You do not need to run the above command if you run the `archive` command from the Console.

Standalone `archive` Command Syntax:

```
arcsight archive -standalone -f Filename [-i | -sort] [-q] ...
```

**Note**

Both remote and standalone `archive` commands support the same optional arguments.

See the description for the `archive` command in [Appendix A, , on page 99](#) for more information on this tool.

## Exporting Resources to an Archive

- 1 Open a shell window or a Windows command prompt window, on a computer where either ArcSight Console or ArcSight Manager is installed.

**Caution**

If you are on the computer where ArcSight Manager is installed, and are running the archive command in remote mode for the first time, go to the `<ARCSIGHT_HOME>/bin` directory and type the following:

```
arcsight tempca -ac
```

This command adds a certificate to the Manager's key store for secure SSL communication with the ArcSight Manager.

**Note**

From the `<ARCSIGHT_HOME>/bin` directory, you can enter the command, `arcsight archive -h` to get help. In that case, the command displays a list of parameters you can specify with the `archive` command.

- 2 From the `<ARCSIGHT_HOME>/bin` directory, enter the `arcsight archive` command along with any parameters you want to specify. For example (on Windows):

```
arcsight archive -u admin -p password -m hostname
-f c:\archive\archive.xml
```

This command first logs into ArcSight Manager. It then displays a list of Resources available for archiving.



Note

If the ArcSight Manager is running, you must specify archive commands in remote mode, entering your user name, password, and Manager name to connect to ArcSight Manager. To run the archive command in standalone mode, accessing resources directly from the ArcSight Database, enter `-standalone` rather than `-u <username> -p <password> -m <manager>`.

- 3 Enter the number of the resource type to archive.

The `archive` command now displays a list of options that let you choose which resource or group of resources within the resource type that you want to archive.

- 4 Choose the resource or group to archive.

After making your selection, you are prompted whether you want to add more resources to the archive.

- 5 You can continue adding additional resources to the archive list. When you've finished, answer no to the prompt

`Would you like to add more values to the archive? (Y/N)`

After it is finished writing the archive file, the archive command returns the command prompt, from which you can enter additional commands or exit.

## Importing Resources from an Archive

- 1 Open a shell window or a Windows command prompt window, on a computer where either ArcSight Console or ArcSight Manager is installed.



Caution

If you are on the computer where ArcSight Manager is installed, and are running the `archive` command in remote mode for the first time, go to the `<ARCSIGHT_HOME>/bin` directory and type the following:

```
arcsight tempca -ac
```

This command adds a certificate to the Manager's key store for secure SSL communication with the ArcSight Manager.

- 2 From the `<ARCSIGHT_HOME>/bin` directory, type `arcsight archive` with its parameters and attach `-i` for import.



Note

If the ArcSight Manager is running, you must specify archive commands in remote mode, entering your user name, password, and Manager name to connect to ArcSight Manager. To run the archive command in standalone mode, accessing resources directly from the ArcSight Database, enter `-standalone` rather than `-u <username> -p <password> -m <manager>`.

- 3 Select one of the listed options if there is a conflict.

Importing is complete when the screen displays `Import Complete`.

## About Importing v3.x Content to a v4.x ESM System

If you import content to an ArcSight ESM v4.x system that was exported from a v3.x system, make sure you are aware of the following:

Do not import system content from an ArcSight ESM v3.x or earlier system to an ArcSight ESM v4.x system. If you do so, it can cause unpredictable consequences on the ArcSight Manager and associated Console clients. The Packages feature in v4.x does not prevent you from importing v3.x system content; therefore, you must be careful when importing content into your v4.x system.



The predefined content with which ArcSight ships is referred to as system content. In ArcSight v3.x, system content was available in System Resource\_Name sub-tree of each resource tree. Additional system content for a few resources was available in the ArcSight System Administration sub-tree. For example, system content for the Rules resource was available in [/All Rules/System Rules](#) and system content for the Assets resource was available in [/All Assets/ArcSight System Administration](#) and [/All Assets/System Assets](#). Refer to the complete list of system content URIs listed below at the end of this section.

---

The above restriction does not apply to the custom content you may have created and archived from an ArcSight ESM v3.x system. You can import any custom content to a v4.x system if it does not reference any v3.x system content.

To identify whether your archived files contain ArcSight ESM v3.x system content, do one of the following:

- Read through the archive XML file to locate the system content URIs.
- Use the `arcsight archive` command with the list option to see the system content URIs:

```
arcsight archive -action list -f <archive file name>
```

To remove/exclude system content from the archived file, run this command from `<ARCSIGHT_HOME>\bin` directory:

```
arcsight archivefilter -source <source_file_name> -xuri  
<system_content_URIs_to_exclude> -f <target_file_name>
```

Here is a complete list of system content URIs that must be excluded before importing custom content from an ArcSight ESM v3.x or earlier system to an ArcSight ESM v4.x system:

```
/All Active Channels  
    /ArcSight Solutions  
    /Site Active Channels  
    /System Active Channels  
/All Field Sets  
    /ArcSight Solutions  
    /Site Field Sets  
    /System Field Sets
```



```
/All Active Lists
  /ArcSight Solutions
  /Site Active Lists
  /System Active Lists
/All Agents
  /ArcSight Administration
/All Assets
  /ArcSight Solutions
  /ArcSight System Administration
  /Site Assets/Disallowed Servers
/All Zones
  /System Zones
/All Networks
  /System Networks/Global
  /Site Networks/Local
/All Locations
  /System Locations/ArcSight
/All Cases
  /ArcSight Solutions
  /System Cases
/All Dashboards
  /ArcSight Solutions
  /ArcSight System Administration
  /Site Dashboards
  /System Dashboards
/All Data Monitors
  /ArcSight Solutions
  /ArcSight System Administration
  /Site Data Monitors
  /System Data Monitors
/All Filters
  /ArcSight Solutions
```

```
/ArcSight System Administration
/
/ Site Filters/Device Type Filters
/
/System Filters
/
/All Partitions/
/
/All Profiles
/
/ ArcSight Solutions
/
/ Site Profiles
/
/ System Profiles
/
/All Reports
/
/ ArcSight Solutions
/
/ System Reports
/
/All Rules
/
/ ArcSight Solutions
/
/ Real-time Rules
/
/ System Rules
/
/All Stages/
/
/All Users
/
/ Administrators
/
/ Default User Groups
```

## Syntax for Performing Common Archive Tasks



Make sure you have read the topic [“About Importing v3.x Content to a v4.x ESM System”](#) on page 192 before you perform any of the tasks listed in this section.

For manual importing, run this command in `<ARCSIGHT_HOME>/bin`:

```
arcsight archive -i -format preferarchive -f <file name>
-u <user> -m <manager hostname>
```

Before performing the import operation, you are prompted for a password to log in to the ArcSight Manager.

For exporting:

```
arcsight archive -f <file name>
-u <user> -m <manager hostname>
```

Before performing the import operation, you are prompted for a password to log in to the ArcSight Manager and use a series of text menus to pick which Resources will be archived.

For scheduled/batch importing:

```
arcsight archive -i -q -format preferarchive  
-f <file name> -u <user>  
-p <password> -m <manager hostname>
```

For scheduled/batch exporting:

```
arcsight archive -u admin -p password -m arcsightserver  
-f somefile.xml -uri "/All Filters/Geographic Zones/West  
Coast"  
-uri "/All Filters/Geographic Zones/East Coast"
```



You can specify multiple URI resources with the URI parameter keyword by separating each resource with a space character, or you can repeat the URI keyword with each resource entry.

---



## Appendix G

# TLS Configuration to Support FIPS Mode

---

This appendix covers the following sections:

[“NSS Tools Used to Configure Components in FIPS Mode” on page 198](#)  
[“Types of Certificates Used in FIPS Mode” on page 198](#)  
[“Using a Self-Signed Certificate” on page 199](#)  
[“Using a Certificate Authority \(CA\) Signed Certificate” on page 199](#)  
[“Some Often Used SSL-related Procedures” on page 212](#)  
[“Setting up Server-Side Authentication” on page 218](#)  
[“Setting up Client-Side Authentication” on page 218](#)  
[“Changing the Password for NSS DB” on page 220](#)  
[“Listing the Contents of the NSS DB” on page 221](#)  
[“Viewing the Contents of a Certificate” on page 221](#)  
[“Setting the Expiration Date of a Certificate” on page 221](#)  
[“Deleting an Existing Certificate from NSS DB” on page 222](#)  
[“Replacing an Expired Certificate” on page 222](#)  
[“Using the Certificate Revocation List \(CRL\)” on page 223](#)

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. A cryptographic module is either a piece of hardware or a software or a combination of the two which is used to implement cryptographic logic. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet the FIPS 140-2 standard.



- Not all ESM versions or ArcSight Express models support the FIPS mode.
- PKCS #11 token support may not be available for all ESM versions and ArcSight Express models.

Refer to the ESM Product Lifecycle Document available on the ArcSight Customer Support website for information on the platforms on which FIPS mode and PKCS #11 Token are supported.

Configuring a component to run in FIPS 140-2 mode, requires that you set up TLS configuration on the component. Since TLS is based on SSL 3.0, we recommend that you

have a good understanding of how SSL works. Please read the section [“Understanding SSL Authentication” on page 34](#) for details on how SSL works.

You have to perform some manual steps to set up the TLS configuration. This appendix serves as a reference for the manual procedures you will need to perform on ArcSight Manager, ArcSight Console, and ArcSight Web.



To configure ArcSight SmartConnectors and ArcSight Logger, refer to their respective documentation.

---

## NSS Tools Used to Configure Components in FIPS Mode

NSS is a cross-platform cryptographic C library and a collection of security tools. ArcSight ESM comes bundled with the following three basic NSS command line tools:

- `runcertutil` - is a certificate and key management tool used to generate key pairs and import and export certificates.



### Notes:

- The `runcertutil` tool currently has a limitation due to which it cannot import the certificate when the NSS DB is set to FIPS mode. In order to work around this issue, you have to disable FIPS mode in the NSS DB first, then import the certificate, and lastly re-enable FIPS mode.
  - When generating a key pair on the Manager or ArcSight Web, it is mandatory to use “mykey” (without quotes) as the alias name for the key pair.
- 

- `runmodutil` - is the NSS module configuration tool. It is used to enable or disable the FIPS module and change Keystore passwords.
- `runpk12util` - is an import and export tool for PKCS #12 format key pairs (.pfx files).

See [Appendix A, ArcSight Commands, on page 99](#) for details on the above command line tools. You can also refer to the ‘NSS Security Tools’ page on the Mozilla website for more details on any of the above NSS tools (make sure to search for them as certutil, modutil, or pk12util).

For online help on any command, enter the following command from a component’s `\bin` directory:

```
arcsight <command_name> -H
```

## Types of Certificates Used in FIPS Mode

You can use either a self-signed certificate or a CA-signed certificate when setting up SSL authentication on your ESM components.

## Using a Self-Signed Certificate

The “Installing ArcSight ESM in FIPS Mode” appendix in the *ArcSight ESM Installation and Configuration Guide* walks you through the steps to generate and use a self-signed certificate when doing a fresh installation of ESM in FIPS mode.

## Using a Certificate Authority (CA) Signed Certificate

In ESM, the Manager and ArcSight Web are both servers. You can use CA-signed certificates for both of them. To use a CA-signed certificate, you have to first obtain the signed certificate from the CA. The CA embeds the public key of the server and the CA's signature in the certificate. So, the Manager's CA-signed certificate will contain the public key of the Manager along with the CA's signature, and the Web's CA-signed certificate will contain the public key of the Web along with the CA's signature.

To obtain the CA-signed certificate, you have to generate a Certificate Signing Request (CSR) on the server (Manager or the Web as the case may be). Next, you send the CSR to the CA. Using the CSR, the CA then creates a certificate for the server and sends it back to you. Once you receive the certificate from the CA, you have to import the certificate into the server's NSS DB.

You are also required to import the server's certificate into any client that wishes to connect to the server. Doing this allows the client to trust the server.

Here are the detailed steps that you will need to perform on each component if you choose to use CA-signed certificates:

### Steps Performed on the Manager



Make sure that your Manager's nssdb does not contain any previously imported/generated Manager certificate or key pair. To confirm this, list all the contents of the nssdb by running the following from the Manager's `/bin` directory:

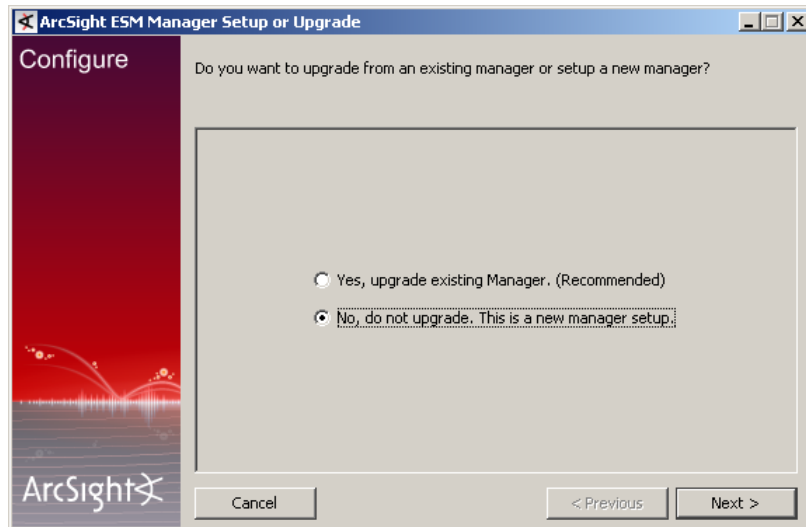
```
./arcsight runcertutil -K -d <ARCSIGHT_HOME>/config/jetty/nssdb
```

If you find a certificate or a key pair in the output of the command, delete it by running the following command:

```
./arcsight runcertutil -D -n <certificate-alias> -d  
<ARCSIGHT_HOME>/config/jetty/nssdb
```

- 1** Install the Manager by running its executable file.

- When you get to the first configuration screen shown below, leave the wizard running and open a command prompt window.



- Generate a key pair on the Manager by running the following from the Manager's `/bin` directory:

```
./arcsight runcertutil -G -d <ARCSIGHT_HOME>/config/jetty/nssdb
```

When prompted for password, enter "changeit" (without the quotes).

Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

```
root@n11-h170:/home/builds
arcsight:/home/arcsight/arcsight/Manager-6391/bin>
arcsight:/home/arcsight/arcsight/Manager-6391/bin>
arcsight:/home/arcsight/arcsight/Manager-6391/bin>./arcsight runcertutil -S -s "CN=<host-
name>" -v 6 -n mykey -k rsa -x -t "C,C,C" -m 1234 -d /home/arcsight/arcsight/Manager-639
1/config/jetty/nssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Manager-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Manager-6391/jre

ArcSight certutil starting...

Enter Password or Pin for "NSS FIPS 140-2 Certificate DB":

A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

|*****|

Finished. Press enter to continue:

Generating key. This may take a few moments...

arcsight:/home/arcsight/arcsight/Manager-6391/bin>
```

- Verify that the key pair got created by entering the following command:

```
./arcsight runcertutil -K -d <absolute_path_to_Manager's_nssdb>
```



Enter "changeit" when prompted for the nssdb password. You should see something similar to `<0> rsa <key>` in the output of the command.

- 5 Generate a CSR by running the following from the Manager's `/bin` directory:

To create a PEM ASCII format CSR file:

```
./arcsight runcertutil -R -s "CN=<hostname_or_IP>,  
O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>,  
ST=<State_where_organization_is_located>, C=<Country>" -a -o  
<absolute_path_to_filename.csr>  
-d <ARCSIGHT_HOME>/config/jetty/nssdb
```



If you do not specify the absolute path to where you want the .csr file to be placed (as shown in the example screen shot below), the .csr file gets placed in the Manager's `<ARCSIGHT_HOME>`.

To create a DER binary file:

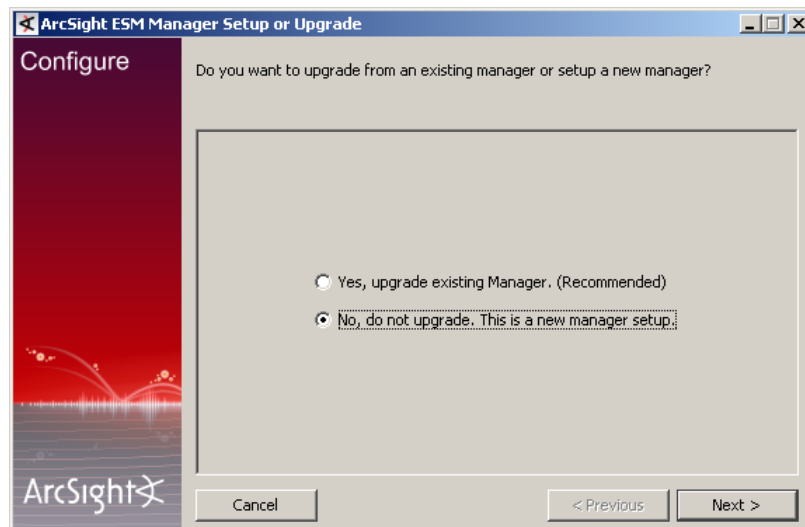
```
./arcsight runcertutil -R -s "CN=<hostname_or_IP>,  
O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>,  
ST=<State_where_organization_is_located>, C=<Country>" -o  
<absolute_path_to_filename.csr>  
-d <ARCSIGHT_HOME>/config/jetty/nssdb
```

Enter the password for the NSS DB when prompted. The default password is "changeit" (without the quotes).

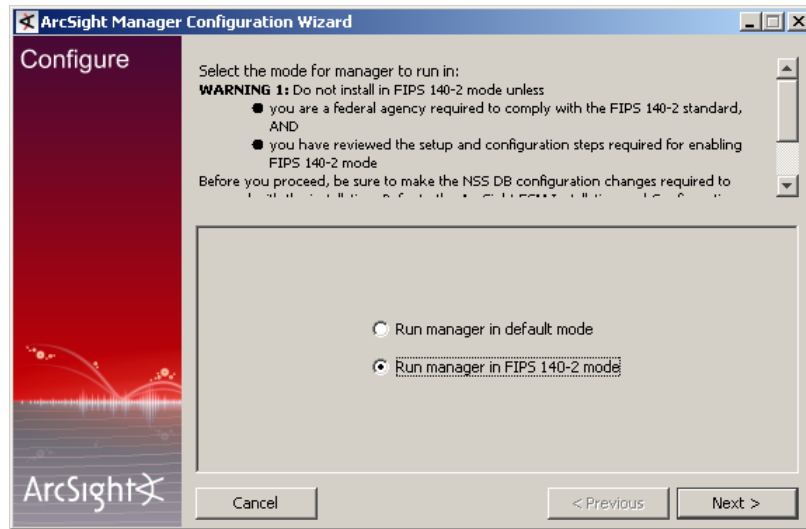
Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

The CSR gets generated in the location specified by the -o option.

- 6 Go back to the installation wizard screen and choose **No, do not upgrade. This is a new manager setup** to create a new, clean installation and click **Next**.

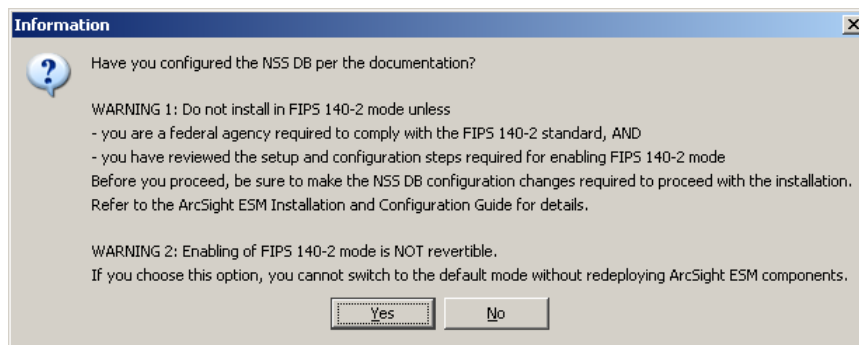


- 7 Next, you will see the following screen:

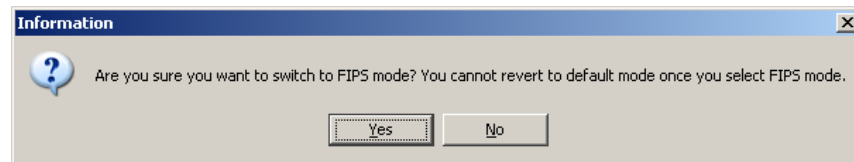


Select the **Run manager in FIPS 140-2 mode** radio button and click **Next**.

- 8 The configuration wizard will ask you to confirm that you have set up the NSS DB. Click **Yes**.



- 9 You will be reminded that once you select the FIPS 140-2 mode, you will not be able to revert to the default mode. Click **Yes**.



- 10 Follow the prompts in the next few wizard screens to complete the Manager installation. Refer to "Installing ArcSight Manager" chapter in the *ArcSight ESM Installation and Configuration Guide* for details on any screen.

- 11 Send the `.csr` file to your Certificate Authority.

The Certificate Authority will send you the signed Manager's certificate which contains the CA's signature and the Manager's public key.

- 12 After you receive the signed certificate from the CA, import it into the Manager's NSSDB by running these commands from the Manager's `/bin` directory:

- a Disable FIPS mode by running:

```
./arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

- b** Import the Manager's CA-signed certificate that you received from your CA by running:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert>
-t "CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/nssdb -i
<absolute_path_to_the_signed_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- c** Enable FIPS mode by running:

```
./arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

- 13** Start the Manager.

## Steps Performed on the Web



- Make sure that you have copied the Manager's certificate to the machine on which you will be installing ArcSight Web.
- Make sure that your Web's webnssdb does not contain any previously imported/generated certificate(s) or key pair(s). To confirm this, list all the contents of the webnssdb by running the following from the Web's `/bin` directory:

```
./arcsight runcertutil -K -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

If you find a certificate or a key pair in the output of the command, delete it by running the following command:

```
./arcsight runcertutil -D -n <certificate-alias> -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

ArcSight Web plays a dual role. On one hand, it acts as a client to the Manager to which it connects. On the other, it acts as a server to web browsers that connect to it. Therefore, the Web authenticates the Manager but has to authenticate itself to web browsers.

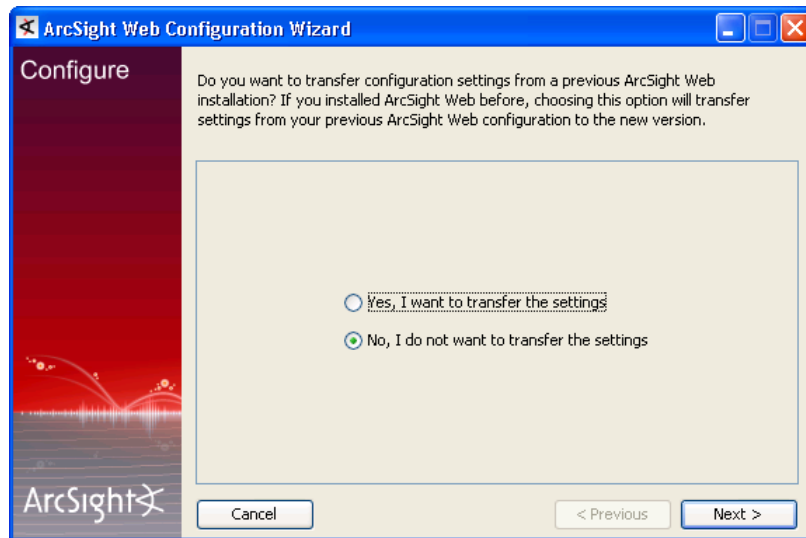
To authenticate the Manager, the Web's NSS DB should contain the Manager's certificate. At the same time, since the Web acts as a server to the web browsers that connect to it, you should have a key pair and a certificate containing the Web's public key in the Web's NSS DB. This allows the Web to authenticate itself to the web browsers.

So, you will be required to import the Manager's certificate into the Web's `webnssdb`. To obtain a CA-signed certificate for the Web, you have to generate a key pair on the Web, generate a CSR on the Web, and send the CSR to the CA. Lastly, after you receive the signed certificate from the CA, import it into the `webnssdb`.

To accomplish all of the above:

- 1** Install ArcSight Web by running its executable file.

- 2 When you get to the first configuration screen shown below, leave the wizard running and open a command prompt window.



- 3 Import the Manager's certificate:
  - a Disable FIPS mode in the Web's `webnssdb`. This is required in order to import certificates into the `webnssdb`.

```
./arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

```
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runmodutil -fips false -dbdir /h
ome/arcsight/arcsight/Web-6391/config/jetty/webnssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

FIPS mode disabled.
arcsight:/home/arcsight/arcsight/Web-6391/bin>
```

- b Import the Manager's certificate into the `webnssdb` by running the following from the Web's `\bin` directory.

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert>
-t "CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_the_Manager's_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

This is required in order for the Web to be able to authenticate the Manager.

```
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runcertutil -A -n ManagerCert -t
"CT,C,C" -d /home/arcsight/arcsight/Web-6391/config/jetty/webnssdb -i /home/arcsight/arcsight/Manager-6391/ManagerCert.cer

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight certutil starting...

arcsight:/home/arcsight/arcsight/Web-6391/bin>
```

- c Enable FIPS mode by running:

```
./arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

```
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runmodutil -fips true -dbdir /home/arcsight/arcsight/Web-6391/config/jetty/webnssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

FIPS mode enabled.
arcsight:/home/arcsight/arcsight/Web-6391/bin>
```

- 4 Generate a key pair on the Web by running:

```
./arcsight runcertutil -G -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

Enter the password for `webnssdb` when prompted. The default password is 'changeit' without the quotes.

Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

```
arcsight:/home/arcsight/arcsight/Web-6391/bin>
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runcertutil -S -s "CN= <hostname>" -v 6 -n mykey -k rsa -x -t "C,C,C" -m 9876 -d /home/arcsight/arcsight/Web-6391/config/jetty/webnssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight certutil starting...

Enter Password or Pin for "NSS FIPS 140-2 Certificate DB":

A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

|*****|

Finished. Press enter to continue:

Generating key. This may take a few moments...

arcsight:/home/arcsight/arcsight/Web-6391/bin>
```

- 5 Verify that the key pair got created by entering the following command:

```
./arcsight runcertutil -K -d <absolute_path_to_Web's_webnssdb>
```

Enter "changeit" when prompted for the webnssdb password. You should see something similar to `<0> rsa <key>` in the output of the command.

- 6 Generate a CSR in the `webnssdb` which you have to send to the CA to obtain a CA-signed certificate for the Web:

```
./arcsight runcertutil -R -s "CN=<hostname_or_IP>,  
O=<company_name>, L=<Location_of_the_company>,  
ST=<State_where_company_is_located>, C=<country>" -a -o  
<absolute_path_to_the_filename.csr> -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

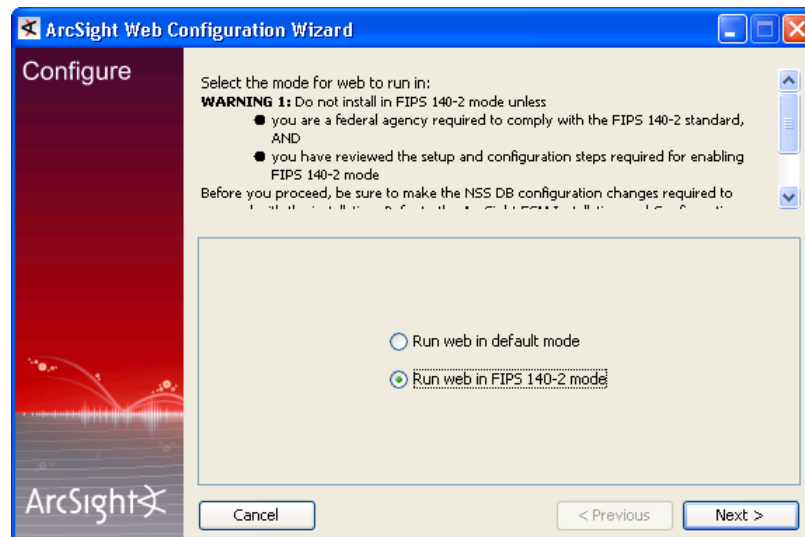


#### Notes:

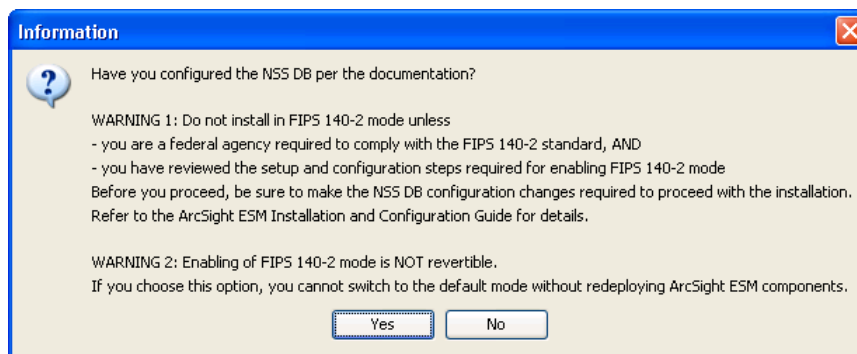
- Make sure the CN is either the IP address of the machine on which ArcSight Web resides or its fully qualified domain name that will be used in the URL when you access ArcSight Web using a browser.
- If you do not specify the absolute path to where you want the `.csr` file to be placed, the `.csr` file gets placed in the Web's `<ARCSIGHT_HOME>`.

This will generate a CSR file which will be placed in the location that you had specified in the `-o` option in the command.

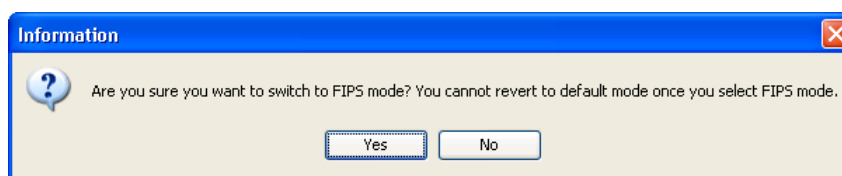
- 7 Go back to the wizard screen. Select **No, I do not want to transfer the settings** and click **Next**.
- 8 Select **Run web in FIPS 140-2 mode** in the following screen and click **Next**:



- 9 You will see the following prompt asking you whether you configured your [webnssdb](#). Click **Yes**.

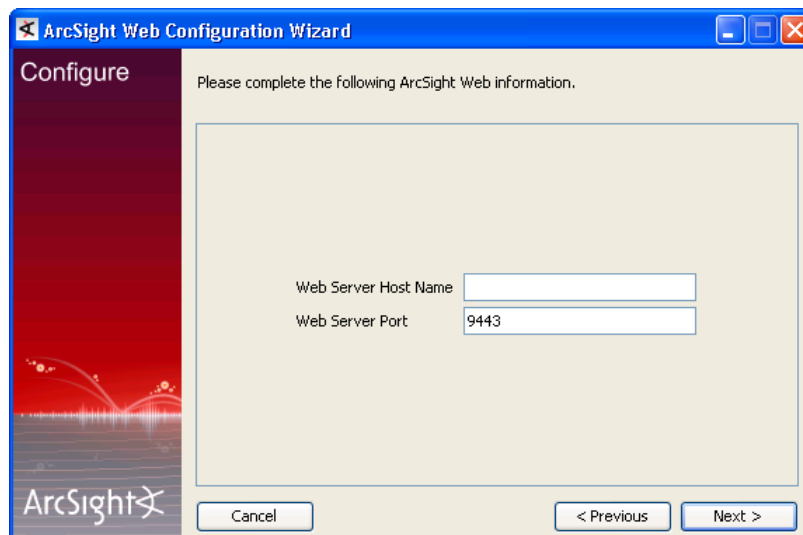


- 10 You will see this warning message:



Click **Yes**.

- 11 When you get to the following screen, make sure that the Webserver Host name exactly matches the host name that you had entered for the webserver when installing the Manager. For example, if you had entered an IP address for the webserver in the Manager setup, make sure to enter the IP address in this screen too.



- 12 Follow the prompts in the next few wizard screens and complete the wizard.

- 13 Send the .csr file to your Certificate Authority.

The Certificate Authority will send you the signed Web's certificate which contains the CA's signature and the Web's public key.

- 14 After you receive the Web's signed certificate from the CA, import it into the Web's [webnssdb](#).

- a** Disable FIPS mode on the webserver by running the following command from the Web's `/bin` directory:

```
./arcsight runmodutil -fips false -dbdir  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

- b** Import the Web's CA-signed certificate by running:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert>  
-t "CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i  
<absolute_path_to_the_web_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

---

The web browsers that connect to the webserver use the Web's certificate to authenticate the webserver.

- c** Enable FIPS mode by running the following from the Web's `/bin` directory:

```
./arcsight runmodutil -fips true -dbdir  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

- 15** Start ArcSight Web by running the following from its `/bin` directory:

```
./arcsight webserver
```

## Steps Performed on the Console

You are required to import the Manager's certificate into the Console's `nssdb.client`. This allows the Console to trust the Manager.



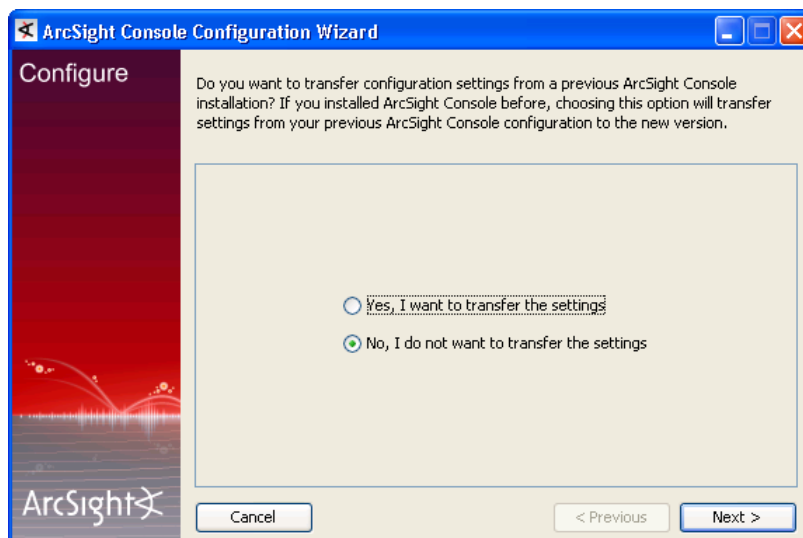
Make sure that you have copied the Manager's certificate to the machine on which you will be installing ArcSight Console.

---

- 1** Install the Console by running its executable file.



- 2 When you get to the first configuration screen shown below, leave the Console running and open a command prompt window.



- 3 Import the Manager CA certificate CA's root certificate which you can obtain from the CA that signed the Manager's certificate:

- a Set the Console's `nssdb.client` temporarily to non-FIPS 140-2 mode by running the following command from the Console's `<ARCSIGHT_HOME>\current\bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

```

C:\arcsight\Console\current\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Console\current\config\nssdb.client

Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause corruption of your security databases. If the browser is currently running, you should exit browser before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode disabled.
Exiting...
C:\arcsight\Console\current\bin>

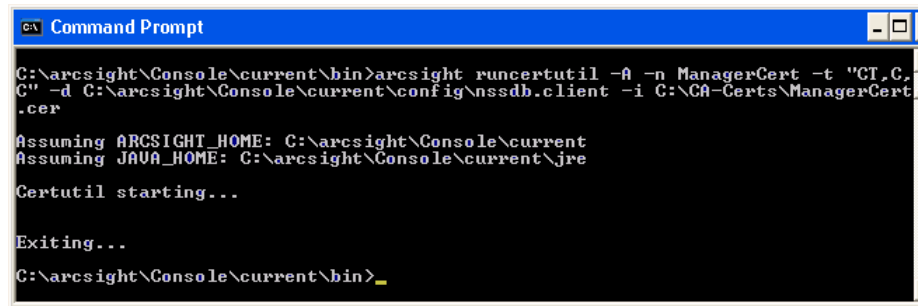
```

- b Run the following command to import the CA's root certificate:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert>
-t "CT,C,C" -d <ARCSIGHT_HOME>\current\config\nssdb.client -
i <path_to_the_CA's_root_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.



```
C:\arcsight\Console\current\bin>arcsight runcertutil -A -n ManagerCert -t "CT,C,C" -d C:\arcsight\Console\current\config\nssdb.client -i C:\CA-Certs\ManagerCert.cer

Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre

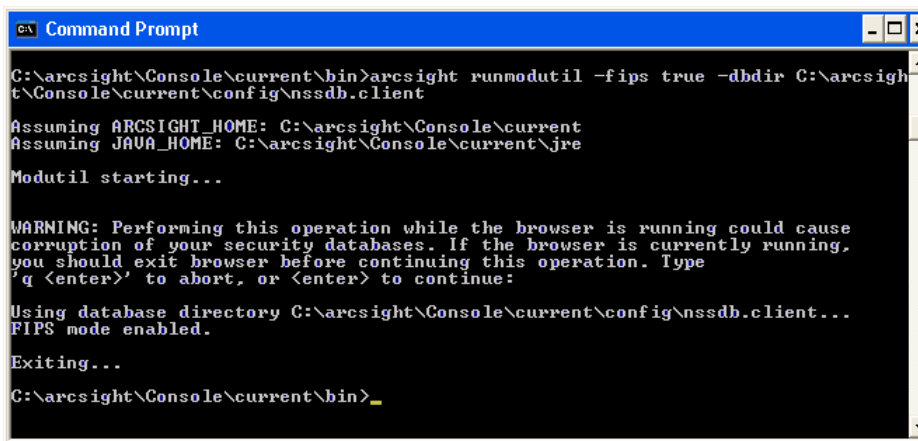
Certutil starting...

Exiting...

C:\arcsight\Console\current\bin>
```

- c Run the following command to enable FIPS mode in `nssdb.client`:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\nssdb.client
```



```
C:\arcsight\Console\current\bin>arcsight runmodutil -fips true -dbdir C:\arcsight\Console\current\config\nssdb.client

Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre

Modutil starting...

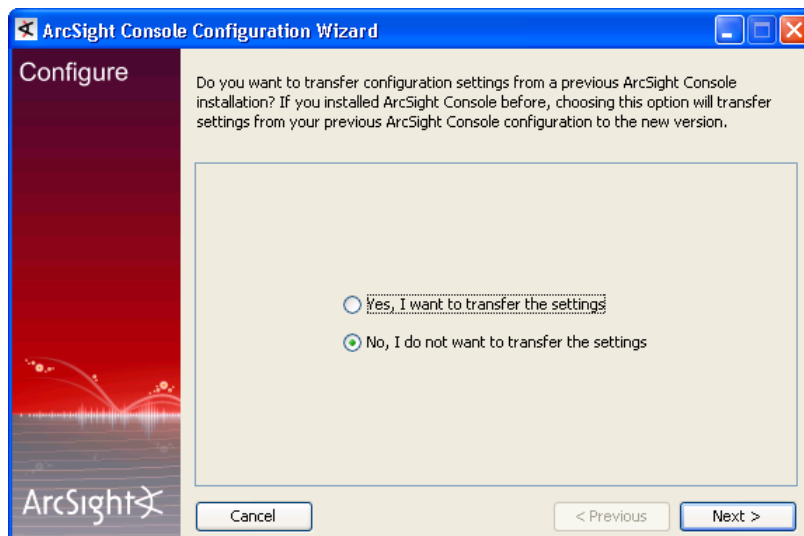
WARNING: Performing this operation while the browser is running could cause corruption of your security databases. If the browser is currently running, you should exit browser before continuing this operation. Type 'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode enabled.

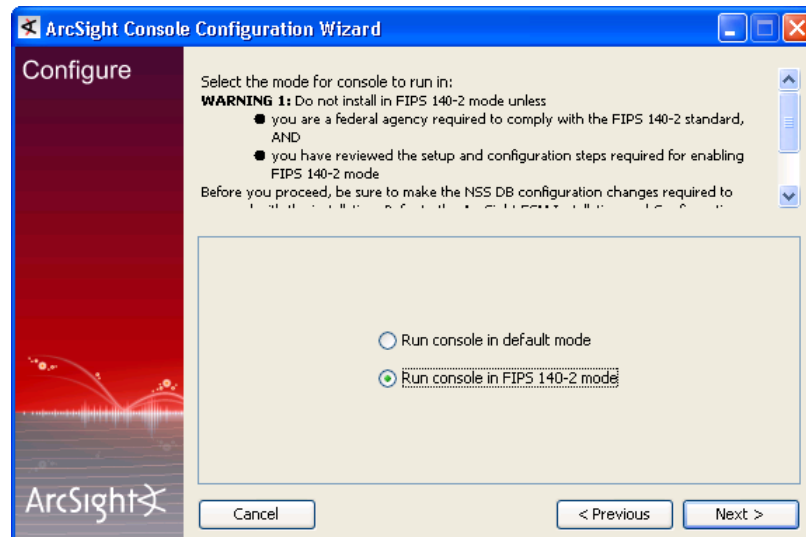
Exiting...

C:\arcsight\Console\current\bin>
```

- 4 Go back to the wizard and select **No, I do not want to transfer the settings** in the following screen and click **Next**:

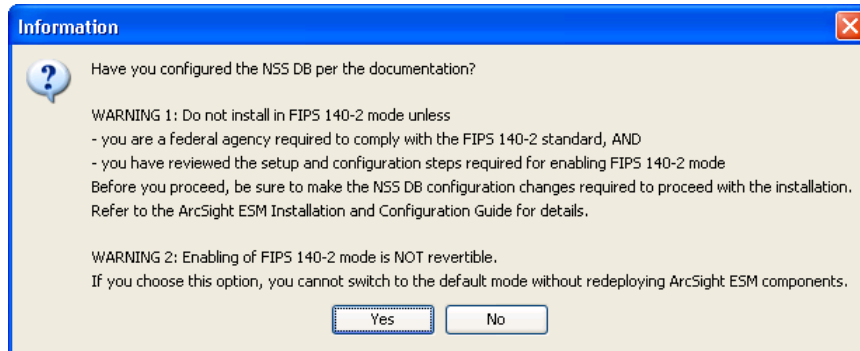


- 5 Next, you will see the following screen:

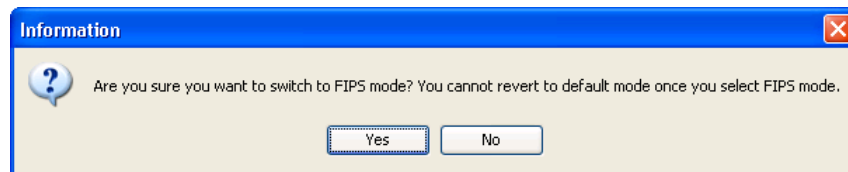


Select **Run console in FIPS 140-2 mode** and click **Next**.

- 6 The configuration wizard will remind you to set up the NSS DB. Click **Yes**.

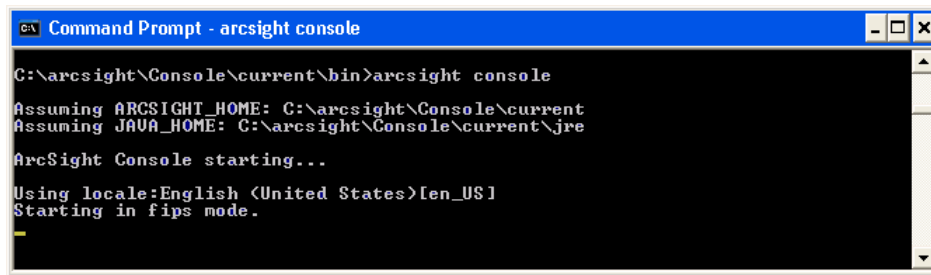


- 7 You will be reminded that once you select the FIPS 140-2 mode, you will not be able to revert to the default mode. Click **Yes**.



- 8 Follow the prompts in the next few wizard screens to complete the Console installation. Refer to "Installing ArcSight Console" chapter in the *ArcSight ESM Installation and Configuration Guide* for details on any screen.

When you start the Console. You should see a message saying that the Console is starting in FIPS mode, as shown in the screenshot below.



```

C:\arcsight\Console\current\bin>arcsight console
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
ArcSight Console starting...
Using locale:English <United States>[en_US]
Starting in fips mode.

```

## Some Often Used SSL-related Procedures

Here are some of the commonly used SSL-related procedures that are intended to serve as a reference when installing or setting up ESM components in FIPS mode.

### Generating a Key Pair in a Component's NSS DB



Note

When you import or generate a key pair in a component's NSS DB, if there is a existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility will use the existing alias for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

This section explains how to generate a key pair in a component's NSS DB. A component that has to authenticate itself is required to have a key pair on it. For example, during server-side authentication, since the server needs to authenticate itself to a client, the server should have a key pair in its NSS DB and send its certificate which contains the server's public key to the client requesting it. The same is true for client-side authentication where a key pair has to exist on the client. For self-signed certificate, the certificate gets generated when generating a key pair.

### On the Manager

- 1 Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory to generate a key pair:

```

./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey -k
rsa -x -t "C,C,C" -m 1234 -d <ARCSIGHT_HOME>/config/jetty/nssdb

```



Caution

For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.



Note

- Make sure to use “mykey” (without quotes) as the alias name for the key pair as shown in the example.
- The `-m` serial number should be unique within `nssdb`
- The hostname is the short name or fully qualified domain name depending upon how your ESM manager name was set up when you installed the Manager.
- Using `-v` to set the validity period of your certificate is optional. If you do not use this option, the certificate will be valid for 3 months by default. Using `-v` is optional. If you choose to use it, see [“Setting the Expiration Date of a Certificate” on page 221](#) for details.

where the hostname is the name of the machine on which your Manager is installed and `-v` is the validity period of the certificate.

For example, if your hostname is `myhost.arcsight.com`, you would run:

```
./arcsight runcertutil -S -s "CN=myhost.arcsight.com" -v 6 -n
mykey -k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/nssdb
```

This will generate a key pair and certificate with the alias `mykey` which is valid for 6 months from the current date and time in the Manager's `nssdb`.

- 2 Enter the password for NDSS DB when prompted. The default password is “changeit” (without the quotes).
- 3 Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

## On the Console

To create a key pair on the Console:

- 1 Run the following command from the Console's `\bin` directory:

```
arcsight runcertutil -S -s "CN=<External_ID_of_the_user>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey -k
rsa -x -t "C,C,C" -m 4975 -d
<ARCSIGHT_HOME>\current\config\nssdb.client
```



Caution

For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.



Note

- Make sure to use `mykey` as the alias.
- CN is the External ID of the user you created when running the Manager's setup.
- The `-m` serial number should be unique within `nssdb.client`.
- Using `-v` is optional. If you choose to use it, see [“Setting the Expiration Date of a Certificate” on page 221](#) for details.

- 2 Enter the password for `nssdb.client`. The default password is ‘changeit’ without quotes.
- 3 Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

## On ArcSight Web

To create a key pair on the Web server:

- 1 Run the following command from ArcSight Web's `/bin` directory:

```
./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey -k
rsa -x -t "C,C,C" -m 2345 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```



For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.

2345 represents the serial number which has to be unique within the `webnssdb` and `hostname` is the name of the machine on which ArcSight Web is installed.



### Notes:

- Make sure to use the alias `mykey`.
- Make sure that this serial number is different from the serial number used when you generated the Manager's key pair. Since the Manager's certificate gets imported into the `webnssdb`, you need to make sure that the serial number for the Web's key pair is different from the serial number used when generating the Manager's key pair.
- Using `-v` is optional. If you choose to use it, see ["Setting the Expiration Date of a Certificate" on page 221](#) for details.

- 2 Enter the password for `webnssdb`. The default password is 'changeit' without the quotes.
- 3 Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

## Verifying Whether the Key pair Has Been Successfully Created

To verify whether the key pair has been successfully created in the `nssdb`, run the following from the component's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -d <path_to_the_component's_NSS_DB>
```



When you import or generate a key pair into NSS DB, if there is a existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility will use the existing alias for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

## Viewing the Contents of the Certificate

If you would like to check the contents of the certificate, you run this from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <path_to_the_component's_NSS_DB> -
n <key_alias>
```

## Exporting a Certificate

This section explains how to export a certificate from a component's NSS DB. During an SSL handshake, for server side authentication, you need to have the server's certificate in the NSS DB of both the server and the client. So, you will need to export the server's certificate from the server's NSS DB in order to import it into the client that wishes to connect to the server.

Likewise, for client side authentication, you need to have the client's certificate in the NSS DB of both the client and the server. So, you will need to export the client's certificate from the client's NSS DB in order to import it into the server that the client will be connecting to.

### From the Manager

Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o
<absolute_path_to_where_you_want_certificate_exported>
```

For example:

```
./arcsight runcertutil -L -n managercert -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o
/home/arcsight/arcsight/Manager-6391/ManagerCert.cer
```

This will export the Manager's certificate into a file called ManagerCert.cer and place it in your `/home/arcsight/arcsight/Manager-6391` directory. The alias for this file will be managercert.



If you do not specify the absolute path for the `.cer` file, it gets placed in the Manager's `<ARCSIGHT_HOME>`.

Note

### From the Console

To export the Console's certificate run the following from the Console's `\bin` directory:

```
arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d
<ARCSIGHT_HOME>\current\config\nssdb.client -o
<absolute_path_to_where_you_want_certificate_exported>
```



If you do not specify the absolute path for the `.cer` file, it gets placed in the Console's `<ARCSIGHT_HOME>`.

Note

### From the Web

To export the Web's certificate, run the following from the Web's `/bin` directory:

```
./arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb -o  
<full_path_to_where_you_want_certificate_exported>
```



If you do not specify the absolute path for the `.cer` file, it gets placed in the Web's `<ARCSIGHT_HOME>`.

## Importing a Certificate into NSS DB

This section explains how to import a certificate into a component's NSS DB. For server side authentication, the server's certificate needs to be imported into the client's NSS DB. For client side authentication, the client's certificate needs to be imported into the server's NSS DB.

The NSS tool, `certutil`, is used to import a certificate into the NSS DB. The `certutil` tool currently has a limitation that it cannot import the certificate when the component is running in FIPS mode. In order to work around this issue, you have to disable FIPS mode on the component first, then import the certificate, and lastly re-enable FIPS mode.

### On the Manager

If you use a CA-signed certificate, you will be required to import the Manager's CA-signed certificate into the Manager's `nssdb`. In addition, if you set up client side authentication, you will be required to import the client's certificate into the Manager's `nssdb`. To import a certificate into the Manager's `nssdb`:

- 1 Disable FIPS mode by running the following from the Manager's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runmodutil -fips false -dbdir  
<ARCSIGHT_HOME>/config/jetty/nssdb
```

- 2 Run the following to import the certificate into the Manager's `nssdb`:



If you are importing the Console's certificate to set up client-side authentication, make sure that you do NOT use the alias `mykey` for the Console's certificate when importing it into the Manager's `nssdb` because the `nssdb` already has the Manager's certificate with the alias `mykey` in it. All aliases in the `nssdb` should be unique.

```
./arcsight runcertutil -A -n  
<provide_an_alias_for_the_certificate> -t "CT,C,C" -d  
<ARCSIGHT_HOME>/config/jetty/nssdb -i  
<absolute_path_to_the_certificate_file>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 3 Run the following command to re-enable the FIPS 140-2 mode:

```
./arcsight runmodutil -fips true -dbdir  
<ARCSIGHT_HOME>/config/jetty/nssdb
```



## On the Console

You are required to import the Manager's certificate into the Console that will be connecting to the Manager. To import a certificate into the Console's `nssdb.client`:

- 1 Set the `nssdb` temporarily to non-FIPS 140-2 mode by running the following from the Console's `<ARCSIGHT_HOME>\bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

- 2 Run the following to import the certificate:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\config\nssdb.client -i
<absolute_path_to_certificate_file>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 3 Run the following command to set the `nssdb` back to FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

## On ArcSight Web

To import a certificate on ArcSight Web:

- 1 Run the following from ArcSight Web's `<ARCSIGHT_HOME>/bin` directory to temporarily disable the FIPS 140-2 mode in order to import the certificate:

```
./arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

- 2 Run the following to import the Manager's certificate into ArcSight Web's `webnssdb`:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_the_certificate_file>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 3 Run the following to re-enable the FIPS 140-2 mode:

```
./arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

## Importing an Existing Key Pair into the NSS DB

If you already have an existing key pair, you can use it instead of generating a new key pair on a component. This procedure instructs you how to import an existing key pair into a component's NSS DB.

- 1 Export the key pair using a tool, such as `keytoolgui`, and be sure to export the key pair with the name `mykey.pfx`. An alias is required in order to import the key pair into NSS DB.
- 2 Import the `.pfx` file into NSS DB using the `pk12util` tool. Make sure that the alias of the key pair being imported does not match the alias of a pre-existing key pair in the component's NSS DB. If the key pair being imported has an alias that matches a pre-existing key pair, the key pair will fail to import citing an error:

```
PKCS12 decode validate bags failed: The user pressed cancel.
```

Run the following command from the component's `/bin` directory:

On the Manager:

```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d  
<ARCSIGHT_HOME>/config/jetty/nssdb
```

On the Web:

```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

On the Console:

```
arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d  
<ARCSIGHT_HOME>\current\confignssdb.client
```

- 3 Run the following from the component's `<ARCSIGHT_HOME>/bin` directory to verify that the key pair has been imported correctly. Note that the alias of the key pair that you just imported in the NSS DB will be the same as the alias of that key pair in the `.pfx` file, in our example, `mykey`.

On Manager:

```
./arcsight runcertutil -L -d <ARCSIGHT_HOME>/config/jetty/nssdb
```

On Web:

```
./arcsight runcertutil -L -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

You should see the alias of the imported key pair in the output.

## Setting up Server-Side Authentication

When you install a component in FIPS mode, you set it up for server-side authentication. Setting up client-side authentication is optional.

The *ArcSight ESM Installation and Configuration Guide* walks you through the steps for installing ESM with server-side authentication.

## Setting up Client-Side Authentication

SSL 3.0 supports client-side authentication. TLS is based on SSL 3.0. ArcSight ESM uses TLS and supports client-side authentication.

The client side authentication takes place after the initial handshake (after the Manager has authenticated itself to the Console). The Manager then requests the Console for its (Console's) certificate. The Console in turn sends its certificate to the Manager. The Manager has to be configured to accept the Console's certificate. In other words, the

Console's certificate must exist in the Manager's `nssdb` prior to the Manager authenticating the Console. With this high level overview in mind, here are the steps you need to perform to set up client-side authentication.

If you plan to use self-signed certificate for the Console:

- 1 Stop the Console if it is running.
- 2 Generate a key pair in the Console's `nssdb.client`. Follow the steps in ["Generating a Key Pair in a Component's NSS DB" on page 212](#) ("On the Console" subsection). This will automatically generate a self-signed certificate on the Console's NSS DB.

Alternatively, you can use an existing key pair which you have to import into the Console's NSS DB. See ["Importing an Existing Key Pair into the NSS DB" on page 217](#) for details.

- 3 Export the Console's certificate. See the section ["Exporting a Certificate" on page 215](#) ("From the Console" subsection) for detailed instructions.
- 4 Stop the Manager if it is running.
- 5 Import the Console's certificate into the Manager's `nssdb`. See the section ["Importing a Certificate into NSS DB" on page 216](#) ("On the Manager" subsection) for details.



**Caution**

Make sure that you do NOT use the alias `mykey` for the certificate when importing it into the Manager's `nssdb` because the `nssdb` already has the Manager's certificate with the alias `mykey` in it. All aliases in the `nssdb` must be unique.

- 6 Restart the Manager, then Console.

If you plan to use CA-signed certificate for the Console:

- 1 Stop the Console if it is running.
- 2 Generate a key pair on the Console. See the ["Generating a Key Pair in a Component's NSS DB" on page 212](#) for details.
- 3 Generate a CSR on the Console by running the following from the Console's `\bin` directory:

```
arcsight runcertutil -R -s "CN=<hostname_or_IP>,  
O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>,  
ST=<State_where_organization_is_located>, C=<Country>" -a -o  
<absolute_path_to_filename.csr>  
-d <ARCSIGHT_HOME>\current\config\nssdb.client
```



**Note**

If you do not specify the absolute path to where you want the `.csr` file to be placed, the `.csr` file gets placed in the Console's `<ARCSIGHT_HOME>`.

- 4 Send the CSR file to your CA and obtain a signed certificate from your CA.
- 5 Import the CA-signed certificate into the Console's `nssdb.client`. See ["Importing a Certificate into NSS DB" on page 216](#) (subsection "On the Console") for details.
- 6 Stop the Manager if it is running.

- 7 Import the Console's CA-signed certificate into the Manager's `nssdb`. See ["Importing a Certificate into NSS DB" on page 216](#) (subsection "On the Manager") for details.

## Changing the Password for NSS DB

ESM ships with a default password for the NSS DB, "changeit" (without quotes). ArcSight recommends that you change the password on each component before moving to a production environment. To do so:

- 1 Disable the FIPS mode in NSS DB by running the following from the component's `/bin` directory:

```
./arcsight runmodutil -fips false -dbdir  
<absolute_path_to_the_component's_NSS_DB>
```

- 2 Run the following to list the NSS DB's token name:

```
./arcsight runmodutil -list -dbdir  
<absolute_path_to_the_component's_NSS_DB>
```

- 3 Change the token's password by running the following from the component's `/bin` directory:

```
./arcsight runmodutil -changepw "<name_of_token>" -dbdir  
<absolute_path_to_the_component's_NSS_DB>
```

- 4 Enter the old password and a new password and confirm it when prompted.

- 5 Re-enable FIPS mode on the NSS DB:

```
./arcsight runmodutil -fips true -dbdir  
<absolute_path_to_the_component's_NSS_DB>
```

- 6 Open the properties file:

On the Manager:

Located in: `<ARCSIGHT_HOME>/config/server.properties`.

Change

```
server.privatekey.password.encrypted=<encrypted_password>
```

to

```
server.privatekey.password=<new_unencrypted_password>
```

On the Console:

Located in `<ARCSIGHT_HOME>/current/config/console.properties`

Change

```
console.privatekey.password.encrypted=<encrypted_password>
```

to

```
console.privatekey.password=<new_unencrypted_password>
```

On the Web:

Located in `<ARCSIGHT_HOME>/config/webserver.properties`.

Change

```
webserver.privatekey.password.encrypted=<encrypted_password>
```

to

```
webserver.privatekey.password=<new_unencrypted_password>
```

- 7** Run the setup program from the component's `/bin` directory:

Manager:

```
./arcsight managersetup
```

Console:

```
arcsight consolesetup
```

Web:

```
./arcsight webserversetup
```

and accept all the defaults in the wizard. This is required in order to obfuscate the password that you had entered in plain text.

## Listing the Contents of the NSS DB

After you import a certificate or generate a key pair in a component's NSS DB, you can verify that the certificate import was successful or the key pair has been successfully generated. You can do this by listing the contents of the NSS DB. To view the contents of a component's NSS DB, run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <absolute-path-to-the_component's_NSS_DB>
```

You should see the alias of the certificate you just imported or the alias for the key pair you generated.

## Viewing the Contents of a Certificate

To view the contents of a certificate, run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <absolute-path-to-the_component's_NSS_DB> -n <certificate_alias>
```

## Setting the Expiration Date of a Certificate

To set the expiry date of the certificate, you have to do so when generating the key pair. Once you have generated the key pair, you cannot change the expiration date on the certificate and the certificate will expire in three months by default.

```
./arcsight runcertutil -S -s "CN=<hostname>" -v  
<number_of_months_the_certificate_should_be_valid> -n mykey -k rsa  
-x -t "C,C,C" -m 1234 -d <component's_NSS_DB_path>
```



For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.

You specify the validity of the certificate with the `-v <number_of_months>` option. The value that you provide with `-v` will calculate the number of months that the certificate will be valid starting from the current time. You can use the `-w <offset_months>` along with `-v` to set the beginning time for the validity. The `-w <offset_months>` if used, will calculate the start time of the certificate validity and the offset will be calculated from the current system time. If you do not use the `-w` option, the current time will be used as the start time for the certificate validity. See the subsection, “[runcertutil](#)” in [Appendix A, ArcSight Commands](#), on page 99 for details on the `-v` and `-w` options.

## Deleting an Existing Certificate from NSS DB

To delete a certificate from a component's NSS DB:

- 1 Stop the component if it is running.
- 2 Run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -D -n <certificate-alias> -d <absolute-  
path-to-the_component's_NSS_DB>
```

## Replacing an Expired Certificate

When an existing certificate/nssdb expires on a server (Manager or Web), you need to replace it with a new one. To replace the certificate:

- 1 Stop the server if it is running.
- 2 Delete the expired certificate from the server's NSS DB. See “[Deleting an Existing Certificate from NSS DB](#)” on page 222 for details.

Since the common name (CN) for the new certificate is identical to the CN in the old certificate, you are not permitted to have both the expired as well as the new certificate co-exist in the NSS DB.

- 3 In case of CA-signed certificate, replace the certificate by importing the new certificate into the server's NSS DB.

In case of self-signed certificate, you have to generate a key pair on the server. See “[Generating a Key Pair in a Component's NSS DB](#)” on page 212 for details on how to do this. Generating the key pair automatically generates the certificate.

- 4 On every client that connects to the server, make sure to delete the old expired server certificate from the client's NSS DB and import the server's newly generated certificate.

For example, if your Manager's certificate has expired, you have to

- a Delete the expired certificate from the Manager's `nssdb`.
- b Generate a new key pair (which will automatically generate a new self-signed certificate).
- c Export the newly generated certificate from the Manager.
- d Delete the expired Manager's certificate from the Console's and Web's NSS DB.
- e Import the Manager's new certificate into the Console's and Web's NSS DB.

## Using the Certificate Revocation List (CRL)

Starting in v4.0 SP2, ArcSight ESM supports the use of CRL to revoke a CA-signed certificate which has been invalidated. The CA that issued the certificates also issues a CRL file which contains a signed list of certificates which it had previously issued that it now considers invalid. ArcSight Manager checks the client certificates against the list of certificates listed in the CRL and denies access to clients whose certificates appear in the CRL.

Before you use the CRL feature, make sure:

- Your certificates are issued/signed by a valid Certificate Authority or an authority with an ability to revoke certificates.
- The CA's certificate is present in the Manager's `<ARCSIGHT_HOME>/config/jetty/nssdb` directory  
In the case of client-side authentication, the Manager validates the authenticity of the client certificate using the certificate of the signing CA.
- You have a current CRL file provided by your CA.  
The CA updates the CRL file periodically as and when additional certificates get invalidated.

To use the CRL feature:

- 1 Make sure you are logged out of the Console.
- 2 Copy the CA-provided CRL file into your Manager's `<ARCSIGHT_HOME>/config/jetty/crls` directory.

After adding the CRL file, it takes approximately a minute for the Manager to get updated.

## Migrating an Existing Default Mode ESM Installation to FIPS Mode

You can migrate your existing default mode ESM installation to FIPS mode. Refer to the *ArcSight ESM Installation and Configuration Guide* for details.





## Appendix H

# Monitoring System Health

---

This appendix provides some guidance about some of the configuration you can perform and some of the stock content you can use for monitoring system health. (This appendix does not attempt to list *all* stock content for monitoring system health.)

[“Overview” on page 225](#)

[“ESM Component Configuration” on page 228](#)

[“ESM Content Configuration” on page 229](#)

## Overview

ArcSight ESM performs self-auditing and self-monitoring, using ESM and component event sources. When the ESM, appliances, and SmartConnectors perform certain self-generated system operations (particularly system statistics and health monitoring), they each generate a corresponding event. ArcSight internal events can be leveraged to build content that provides a centralized/unified view of the health of an ArcSight deployment.

This appendix details how to configure various components to send this information to a Manager, allowing comprehensive monitoring of the system health of your ArcSight deployment.

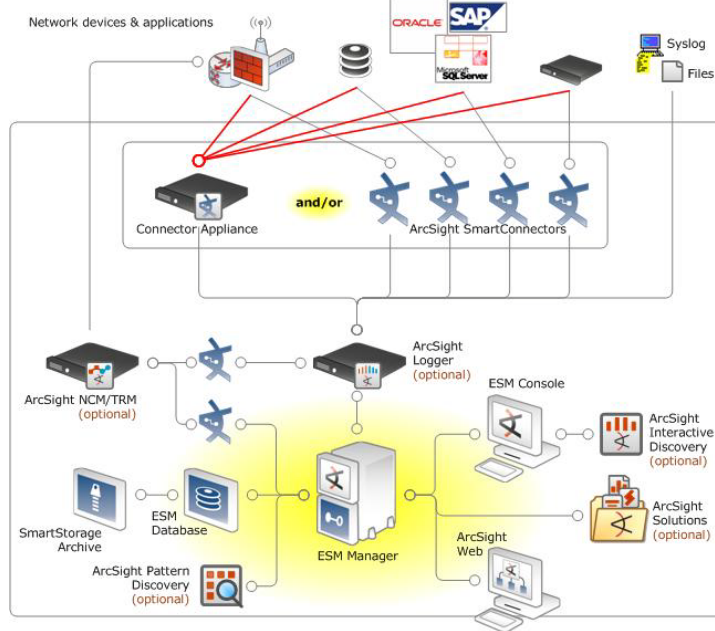
## What to Monitor

Two types of internal events are generated by all ArcSight components:

- Status Monitor Events – periodic statistics about system health such as EPS and database free space.
- Audit Events – Report actions in real time such as user authentication, activity, and resource modification.

For monitoring system health, it is the status monitor event that is of primary concern. You can configure appliances and connectors to forward these events to the Manager. ESM monitors its own local critical system events and the status monitor events sent from components. If any events match its alert criteria (indicating a critical situation), ESM provides a summary of events for further investigation and a drill-down view.

The diagram below is an example of a common scenario that shows the flow of monitor events through an ArcSight appliance ecosystem.



A typical implementation targets the following network elements:

- Availability—Monitor critical devices, ArcSight connectors, appliances, and ESM
- Performance—CPU Usage, memory usage
- Network speed—Current EPS, EPS over time, inbound/outbound traffic
- Disk and Storage—Monitor disk usage and disk free space on appliances and ESM

In monitoring dependent components, ArcSight recommends a focus on the three most typical components: ArcSight SmartConnectors, appliances, and ESM.

## ArcSight Appliances

The internal monitoring events of an ArcSight appliance might monitor CPU usage, memory usage, current EPS, historical EPS, network interface statistics, and available disk usage. The following table shows a subset of appliance internal events that are most relevant for monitoring system health.

### Appliance Internal Events

CPU Statistics	<ul style="list-style-type: none"> <li>• Current value</li> </ul>
Disk Statistics	<ul style="list-style-type: none"> <li>• Disk space</li> <li>• Read/Write</li> </ul>
Event Statistics	<ul style="list-style-type: none"> <li>• EPS (receiver, forwarder)</li> <li>• Event count (receiver, forwarder)</li> </ul>
Memory Statistics	<ul style="list-style-type: none"> <li>• JVM memory</li> <li>• Platform memory</li> </ul>

---

**Appliance Internal Events**


---

Network Statistics	<ul style="list-style-type: none"> <li>• Inbound usage</li> <li>• Outbound usage</li> </ul>
--------------------	---------------------------------------------------------------------------------------------

---

You can find a description of system health events for ArcSight Logger in "Monitoring System Health" in the *ArcSight Logger Administrator's Guide*.

You can find a description of system health events for ArcSight Connector Appliance in "Audit Logs" in the *ArcSight Connector Appliance Administrator's Guide*.

## ArcSight ESM

ArcSight ESM has a number of statistical monitors and alarms for every component of the ArcSight ecosystem. It can monitor SmartConnectors, database performance, resource exhaustion and has a number of reactive mechanisms such as notifications, SNMP forwarding, open cases and executing scripts to deal with system or hardware failures in real time. The following table shows a subset of internal events that are most relevant for monitoring system health. For a list of audit events, see "Audit Events" in the *ArcSight ESM User Guide*.

---

**ESM Internal Events**


---

Resource Statistics	<ul style="list-style-type: none"> <li>• Open resource count</li> <li>• Queries/evaluations per second</li> </ul>
Resource Framework Statistics	<ul style="list-style-type: none"> <li>• Inserts</li> <li>• Updates</li> <li>• Deletes</li> </ul>
Rules Engine Statistics (CPU, memory)	<ul style="list-style-type: none"> <li>• Events in rule engine</li> <li>• Events matching rules</li> <li>• Rate of correlated events</li> </ul>
Event Border Statistics	<ul style="list-style-type: none"> <li>• Event count</li> <li>• Insert time</li> <li>• Retrieval time</li> </ul>
Main Flow Statistics	<ul style="list-style-type: none"> <li>• EPS (count since last monitor event)</li> <li>• Events (count since startup)</li> </ul>
Side Table Statistics	<ul style="list-style-type: none"> <li>• Size</li> <li>• Insert</li> <li>• Cache (misses/hit rate)</li> </ul>
Database Statistics	<ul style="list-style-type: none"> <li>• Free Space</li> <li>• Read/Write</li> </ul>

---

# ESM Component Configuration

## Configuring SmartConnectors

In addition to normalizing and sending compressed events to Logger or ESM, connectors can also monitor the management connection and availability of the originating event sources.

If for some reason ESM or Logger becomes unavailable, a SmartConnector will cache all the data locally, and when connectivity to Logger resumes, send on the events. The following table shows a subset of internal events that are most relevant for monitoring system health.

Connector and Device Events	
Device Statistics	<ul style="list-style-type: none"> <li>• Last event received</li> <li>• Total number of events</li> <li>• Event count Since last call</li> </ul>
Connector Flow Statistics	<ul style="list-style-type: none"> <li>• Event rates</li> <li>• Cache size</li> </ul>
Connector Audit Events	<ul style="list-style-type: none"> <li>• Start/stop</li> <li>• Heartbeat</li> <li>• Cache statistics</li> </ul>

The Connectors for your critical devices should be configured to send the "Connector Device Status" events to the ArcSight Manager periodically. To do this, configure the Connector to enable device status monitoring using the Connectors resource editor.

- 1 In the Navigator panel, go to Connectors and navigate to the Connector you want to configure.
- 2 Right-click the Connector and select **Configure**.
- 3 In the Connector editor in the Inspect/Edit panel, scroll down to the Processing section. In the Enable Device Status Monitoring (in milliseconds) field, enter how often you want the Connector to send Device Status Events.
  - ◆ For example, if the value is set to 300000, the Connector will send status events for all its devices every 5 minutes (300000 milliseconds).
  - ◆ If the value is set to -1, the Connector will send no Device Status events.

For more about enabling device status monitoring and configuring SmartConnectors, see the *ArcSight SmartConnector User's Guide*.

## Configuring the Connector Appliance

To configure the Connector Appliance to forward system health events, you need to add the Syslog Daemon connector to a container, set runtime parameters, and configure audit forwarding on the container. You can skip the steps below that are already done.

- 1 Upload an ESM Certificate to Connector Appliance so that the appliance and Manager can communicate. Refer to the section "CA Certs Repository" in the *ArcSight Connector Appliance Administrator's Guide*.

For information about SSL Authentication and certificates, refer to the section "Understanding SSL Authentication" in the "Configuration" chapter of the *ArcSight ESM Administrator's Guide*.

- 2 Add the ESM certificate to a Container. Refer to the section "Managing Certificates on a Container" in the *ArcSight Connector Appliance Administrator's Guide*.
- 3 Add the Syslog Daemon connector to the container to which you added the certificate. Refer to the section "Adding a Connector" in the *ArcSight Connector Appliance Administrator's Guide*.

When choosing a destination, select ArcSight Manager (encrypted).

- 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 milliseconds) field, to a positive number. The minimum interval is one minute, so use at least 60,000 ms. Smaller values result in one-minute intervals. Entries that are not a positive integer turn the feature off.

See "Editing Destination Runtime Parameters" in the *ArcSight Connector Appliance Administrator's Guide*.

- 5 Configure audit forwarding for the container that has the Syslog Daemon connector. Refer to the section "Audit Forwarding" in the *ArcSight Connector Appliance Administrator's Guide*.

## Configuring Logger

Logger is one of the many appliances from which system health events can be generated, then sent directly to a Manager. To initiate this communication, refer to the "Configuration" chapter in the *ArcSight Logger Administrator's Guide*. The section on "Event Input/Output" describes how to set up Logger to forward events to ESM.



Audit events for alerts are only written to the Internal Storage group and not forwarded to ESM by default. If you need to forward these audit events to ESM, please contact ArcSight Customer Support for assistance. Please note that this change applies only to audit events generated for alerts; other audit events are unaffected.

## Configuring ESM

You can also use a Forwarding Connector to communicate health-related events from a source Manager to a destination Manager, if you have such a hierarchical arrangement. For information, refer to the "Configuration" chapter of the *ArcSight SmartConnector Configuration Guide* for Forwarding Connectors.

## ESM Content Configuration

### Configure Critical Device Not Reporting Resources

The ArcSight Administration content includes resources that monitor the devices in your network and send a notification when one of your critical devices is down. This content

functions off the Device Status events sent by SmartConnectors that you configured in [“Configuring SmartConnectors” on page 228](#).

Resource Type	Universal Resource Identifier (URI)	Resource Name
Filter	/All Filters/ArcSight Administration/Connectors/System Health/Custom/	White List - Devices
Filter	/All Filters/ArcSight Administration/Connectors/System Health/Custom/	White List - Critical Devices
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Device Reported
Rule	/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Reported
Rule	/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/	Reporting Devices

The *Device Reporting* rules reference the White List filters for which devices to track and insert in the *Reporting Devices* active list.



## Configure White List Filters

The *White List - Devices* filter tells the *Devices Reported* rule which devices to track that send Device Status events to the Manager. By default, the condition in the filter is *True*, which means that all the devices that send Device Status events will be inserted in the *Reporting Devices* active list.


Modify this filter to choose only the devices you want to insert in the *Reporting Devices* active list. Entries in this active list never expire.

The *White List - Critical Devices* filter tells the *Critical Device Reported* rule which devices to track that send Device Status events and are also categorized as criticality High ([All Asset Categories/System Asset Categories/Criticality/High](#)).

Modify this filter to choose the critical devices you want to monitor closely and about which you want to be notified when they are not reporting.

The devices in *Reporting Devices* active list are likely to be a subset of the devices in the *Reporting Device* active list. By default, the filter will pick all the assets that are categorized as [All Asset Categories/System Asset Categories/Criticality/High](#). Create conditions that match your critical devices, and categorize your critical assets (or zones) as [All Asset Categories/System Asset Categories/Criticality/High](#).

### To modify the filters to select only the devices you specify:

- 1 In the Navigator panel, navigate to the [White List](#) filters ([All Filters/ArcSight Administration/Connectors/System Health/Custom/](#)) and double-click the one you want to modify to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab.
  - ◆ **White List - Devices filter:** Delete the default condition [True](#) (select the condition and press **Delete**).
  - ◆ **White List - Critical Devices filter:** Leave the Attacker Asset ID and Attacker Zone conditions in place. These identify the asset as being categorized as criticality high.
- 3 Construct an expression that captures the devices you want the rule to evaluate.
  - ◆ **White List - Devices filter:** Select [event1](#) and add an AND operator (click the AND icon ). Use the event fields grid to build the condition, or right-click [event1](#) and select **New Condition**.
  - ◆ **White List - Critical Devices filter:** Select [event1](#) and use the event fields grid to build the condition, or right-click [event1](#) and select **New Condition**.

Depending on the devices you want to capture, you can use device vendor/product, asset categories, and other conditions.



Tip

- **Use Device Custom strings.** You can use Device Custom strings to express device vendor and device product fields. [Device Custom String1](#) is the device vendor (such as Microsoft), [Device Custom String2](#) is the device product (such as Microsoft Windows). For example:  

```
Device Custom String1 = Device Vendor ABC
```

```
Device Custom String2 = Device Product XYZ
```

 (This selects all the devices with that device vendor/product.)
- **Use Attacker fields.** The attacker fields correspond to the device. Use these fields to specify an IP address, a zone or an asset category using the "Attacker" fields, and the appropriate operator. For example:  

```
Attacker Zone = /All Zones/...
```

 (This checks if the device is in a zone.)
- **Use Assets conditions.** Use the Assets condition button to check if a device is in one or more asset categories. For example:  

```
Attacker Asset ID inGroup /All Asset Categories/...
```

- 4 Click **OK** to apply changes and close the Filter editor.

For more about working with the Common Conditions Editor, see the online Help topic *Common Conditions Editor*.

## Configure Critical Device Not Reporting Rule

The *Critical Device Not Reporting* rule is disabled by default. Enable the rule if you want to be notified when one of your critical devices is down. Enable the rule only after you modified the *White List - Critical Devices* filter.

### To enable the rule:

- 1 In the Navigator panel, go to **Rules > All Rules > ArcSight Administration > Connectors > System Health > Custom**.
- 2 Right-click the rule **Critical Device Not Reporting** and select **Enable Rule**.

### To enable the Create New Case action if a critical device goes down:

To create a case when the rule conditions are met, edit the *Create New Case* action to give it an owner and enable the action.

- 1 Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
- 2 In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate user. Click **OK**.
- 3 Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.

## Configure Connector Monitoring Resources

The ArcSight ESM content provides the following resources that monitor the operational status of SmartConnectors configured on the ArcSight Manager, as well as those configured to send events to ArcSight Loggers that are forwarding events to the ArcSight Manager.

Resource Type	Universal Resource Identifier (URI)	Resource Name
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Up
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Down
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Caching
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Caching
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Cache Empty



Resource Type	Universal Resource Identifier (URI)	Resource Name
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Discovered or Updated
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/	Connector Information
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/	Connectors - Down
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/	Connectors - Caching
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/	Black List - Connectors
Active Channel	/All Active Channels/ArcSight Administration/Connectors/System Health/	Connector Connection Status Events
Active Channel	/All Active Channels/ArcSight Administration/Connectors/System Health/	Connector Caching Events
Dashboard	/All Dashboards/ArcSight Administration/Connectors/System Health/	Connector Connection and Cache Status

The *Connector Discovered or Updated* rule monitors all connection and cache status events, whether generated by SmartConnectors or by the ESM Manager. The correlation event from this rule is used by other rules to update connector status.

The following rules are used to identify *connection* status:

- *Connector Down*
- *Connector Up*
- *Connector Still Down*

The following rules are used to identify *caching* status:

- *Connector Caching*
- *Connector Still Caching*
- *Connector Dropping Events*
- *Connector Cache Empty*

The next two sections provide information about configuration options for these rules.

## Configuring Active Lists for Connector Information and Up or Down Status

### Connector Information

The *Connector Information* active list collects information about connectors that have reported into the system, as well as information from the Manager when the SmartConnector is first registered. A SupportInformation column in the list is pre-populated as follows:

'poc= | email= | phone= | dept= | action='.

If you have SmartConnectors that are maintained by other individuals or organizations, you can enter their contact information for each connector.

### Connectors - Down

By default, the attributes for the *Connectors - Down* active list Time to Live (TTL) are set to 20 minutes. A connector down for fewer than 20 minutes is considered to be down for a *short term*.

After 20 minutes, the entry for this active list expires and the connector information is moved to the *Connectors - Still Down* active list, unless the connector comes back up before 20 minutes.

### Connectors - Caching

By default, the attributes for the *Connector - Caching* active list TTL are set to 2 hours. A connector that has been caching for fewer than 2 hours is considered to be caching for a *short term*. Connectors caching for up to 2 hours are not considered to be a problem.

After 2 hours, the entry for this active list expires and the connector information is moved to the *Connectors - Still Caching* active list, unless the connector cache is emptied in fewer than two hours, and it is removed by the *Connector Cache Empty* rule.

## Rules Relating for Connector Up or Down Status

### Connector Up, Connector Down

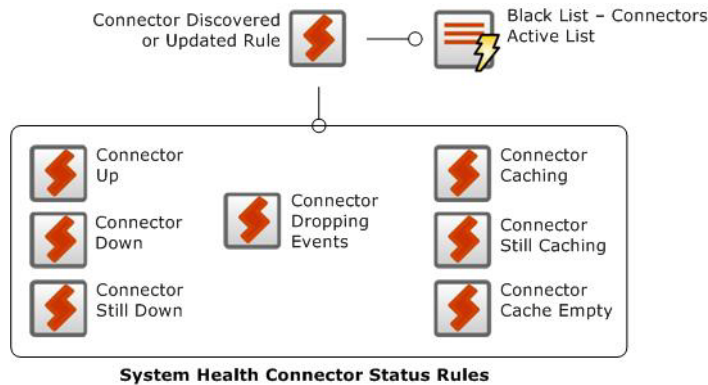
The *Connector Up* and *Connector Down* rules detect SmartConnectors that are started and reporting events, and those that are shut down. These rules can send a notification (if notifications are enabled) when Connectors have been down for a certain period of time (by default, a TTL of 20 minutes in the *Connectors - Down* active list).

### Excluding Some Connectors from Being Evaluated

In some situations, you might want to exclude certain Connectors from being evaluated by the *Connector Up* and *Connector Down* rules:

- You have Connectors that you start and stop manually. For example, if you start a TestAlert connector to replay some events, then stop it when you are done, and you don't want to get a notification saying that the Connector is down every 20 minutes until you restart it.
- After installing and configuring ArcSight, you get unwanted notifications about Connectors going down. You can opt to not receive Connector down notifications from those Connectors.
- You have a Connector scheduled to run once every week (such as a vulnerability scanner), and the Connector is otherwise down in the time in between.
- You are testing a new Connector and you will be starting and stopping it frequently during the set-up process.

For these situations, the *Connector Up* and *Connector Down* rules points to the *Black List - Connectors* active list, as shown in the following figure.



To exclude certain SmartConnectors from being evaluated by these rules, enter the SmartConnector's URI and IP address in the *Black List - Connectors* active list, using the following steps:

- 1 In the Navigator panel, go to **Lists > Active Lists > All Active Lists > ArcSight Administration > Connectors > System Health > Custom**.
- 2 Right-click the active list *Black List - Connectors* and select **Edit Active List**.
- 3 In the Active List Editor in the Inspect/Edit panel, click **Add Entry**.
- 4 In the ActiveList Entry Editor, enter the URI of the SmartConnector (starting with [/All Connectors](#)) and the Connector's IP address and click **Add**, as in the following example:

The screenshot shows the 'ActiveList Entry Editor' window. The 'Active List' is set to 'Black List - Connectors'. The table below shows the entry details:

Name	Value
Connector URI	All Connectors/Site Connectors/Cisco VPN Syslog
Connector Address	111.22.33.0
Creation Time	
Last Modified Time	
Count	1

At the bottom of the window are buttons for 'Modify', 'Add', 'Delete', 'Reset', and 'Cancel'.



You can copy and paste the URI and the IP addresses from the Connector Information active list.

- 5 Repeat steps 3 and 4 for every SmartConnector you want to exclude from the *Connector Up* and *Connector Down* rules.

For more about working with active lists, see the topic *Managing Active Lists* in the *ArcSight ESM User's Guide*.

### Populating Active Lists from an Imported CSV File

- 1 In the Navigator panel, navigate to the active list you want to configure ([Lists > Active Lists](#)).
- 2 Generate a CSV file with the values with which you wish to populate the active list, and save it to a directory on the Console system.
- 3 Right-click the active list you wish to import the values into and select **Import CSV File...**
- 4 In the Open dialog box, navigate to and select the CSV file and click **Open**.

The *Connector Still Down*, *Connector Still Caching*, and *Connector Dropping Events* rules have two actions that are disabled by default:

- Send Notification: Identifies whether an acknowledgement is required, as well as the actual notification text and its destination.
- Create New Case: Specifies the case name, its priority, whether to include the base events, and the group in which the case is included.

These actions are disabled by default because of several possible reasons; for example, users might not have set up notification destinations, users might not have use cases, or the rate of creation might be higher than users prefer.

# Index

---

## A

- About
  - Migrating from one certificate type to another 72
- Adjusting
  - Console Memory 22
- Alphabetic List of Commands 100
- ArcSight Manager
  - Decoupled Process Execution 10
  - Service Setup on Windows 12
- ArcSight Manager or ArcSight Web Service Setup on Unix Platforms 13

## B

- Backing up ArcSight Databases 93

## C

- Changing
  - ArcSight Manager Ports 76
  - Console and ArcSight Web Session Timeouts 76
  - Manager Properties Dynamically 21
  - Oracle Initialization Parameters 91
- Checking Passwords with Regular Expressions 78
- Commonly used elements in Email.vm and Informative.vm files 183
- Comparing Self-signed and CA-signed certificates 46
- Compression and Turbo Modes 84
- Configuring
  - ArcSight Database Monitor 85
  - ArcSight Manager Logging 24
  - ArcSight Manager or ArcSight Web as a Service 12
  - Database Monitor e-mail message recipients 86
  - SNMP trap sender 86
  - the check for free space in Oracle tablespaces 86
- Contents of Email.vm and Informative.vm 184
- Customizing the template files 186

## D

- Database Check Tasks
  - List 171
- Disabling
  - Database Checks 171
- Dynamic Properties 19

## E

- Editing
  - Properties 18
- Enabling
  - Compression for ArcSight SmartConnector

- Events 84

- Enforcing Good Password Selection 76

- Establishing
  - SSL Client Authentication with Login information 57

- Exporting
  - Data 94
  - Resources to an Archive 190

## G

- Gathering
  - logs and diagnostic information 26

## H

- How SSL Works 44
- How the Email.vm and Informative.vm Template Files Work 185

## I

- Importing
  - CA-signed certificate into Manager's key store 54
  - Resources from an Archive 191
  - v3.x Content to a v4.x ESM System 192
- Installing
  - New License Files Obtained from ArcSight 23

## K

- keytool 43
- Keytoolgui 39

## L

- Logfu
  - Example 178
  - Intervals 181
  - Menu 180
  - Typical Data Attributes 180

## M

- Manager
  - Password Configuration 76
- Managing
  - and Changing Properties File Settings 17
- Migrating
  - from Demo to CA-Signed 72
  - from Demo to Self-Signed 72
  - from Self-Signed to CA-Signed 73
- Monitoring Available Free Space in Tablespaces 92

**N**

Notification Velocity templates 183

**O**

Obtaining  
    CA-signed certificate 52  
Oracle  
    Cold Backup 93  
    Hot Backup 93

**P**

Partition logs 95  
Password  
    Length 76  
    Uniqueness 78  
Properties File Settings  
    Defaults and User Properties 17  
Property File Format 17

**R**

Reconfiguring  
    ArcSight Manager 75  
    the ArcSight Console after Installation 75  
Reconnecting to the ArcSight Manager 12  
Recovering ArcSight Databases 94  
Reducing Impact of Anti-Virus Scanning 14  
Re-Enabling User Accounts 80  
Removing the ArcSight Manager Service on Windows 13  
Requiring Mix of Characters in Passwords 77  
Resetting  
    Oracle Password 92  
Restricting Passwords Containing User Name 77  
Restricting the Number of Failed Log Ins 79  
Running  
    ArcSight Command Script 99  
    ArcSight ESM 9  
    Logfu 176

**S**

Securing  
    ArcSight Manager Properties File 22  
Send Logs utility 25  
Sending  
    Events as SNMP Traps 86  
    logs and diagnostic information to ArcSight 25  
Setting  
    Custom Login Message 11

    Database Threshold Notification 92  
    Password Expiration 79  
Speeding up partition compression 94  
SSL certificates 46  
Starting  
    and Stopping the ArcSight Manager Service  
        on Windows 12  
    ArcSight Console 10  
    ArcSight Manager 9  
    ArcSight SmartConnectors 11  
Stopping  
    ArcSight Manager 12  
Syntax for Performing Common Archive Tasks 194

**T**

tempca 44  
Terminology  
    SSL Authentication 35  
The #if statement 183  
Tools for SSL configuration 39  
Troubleshooting  
    ArcSight Web 165  
    Console 162  
    Database 166  
    General 155  
    Logfu 178  
    Manager 164  
    Partition Archiver problems. 162  
    SmartConnectors 161  
    SSL 167  
Types  
    SSL Certificates 46

**U**

Understanding  
    ArcSight Turbo Modes 84  
    Customization Process 185  
    Database Checks 169  
    SSL Authentication 34  
Using  
    CA-Signed Certificate 52  
    Certificates to Authenticate Users to ArcSight 74  
    Demo Certificate 47  
    Self-Signed Certificate 48

**V**

Verifying  
    SSL Certificate Use 73