

# **ArcSight ESM Administrator's Guide**

---

ArcSight™ ESM Version 4.5 SP1

April 21, 2009



## ArcSight ESM Administrator's Guide ArcSight™ ESM Version 4.5 SP1

Copyright © 2009 ArcSight, Inc. All rights reserved. ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. 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/company/copyright/>

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
04/21/09	ArcSight ESM Version 4.5 SP1	Updated screen captures

Document template version: 1.0.2.5

### 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="https://support.arcsight.com">https://support.arcsight.com</a>
Customer Forum	<a href="https://forum.arcsight.com">https://forum.arcsight.com</a>

# Contents

---

<b>About this Guide .....</b>	<b>xiii</b>
Related Documentation .....	xiii
Notes, Tips, and Cautions .....	xiv
Text Conventions .....	xv
Feedback .....	xvi
 <b>Chapter 1: Basic Administration Tasks .....</b>	 <b>1</b>
Running ArcSight ESM .....	2
Starting the ArcSight Manager .....	2
ArcSight Manager Decoupled Process Execution .....	2
Starting the ArcSight Console .....	3
Setting up a Custom Login Message .....	3
Starting ArcSight SmartConnectors .....	3
Stopping the ArcSight Manager .....	4
Reconnecting to the ArcSight Manager .....	4
Configuring ArcSight Manager or ArcSight Web as a Service .....	4
ArcSight Manager Service Setup on Windows .....	4
Starting and Stopping the ArcSight Manager Service on Windows .....	4
Removing the ArcSight Manager Service on Windows .....	5
ArcSight Manager or ArcSight Web Service Setup on Unix Platforms .....	5
Reducing Impact of Anti-Virus Scanning .....	6
 <b>Chapter 2: Configuration .....</b>	 <b>7</b>
Managing and Changing Properties File Settings .....	8
Property File Format .....	8
Defaults and User Properties .....	8
Editing Properties .....	8
Dynamic Properties .....	9
Example .....	10
Changing Manager Properties Dynamically .....	11
Securing the ArcSight Manager Properties File .....	12
Adjusting Console Memory .....	12
Installing New License Files Obtained from ArcSight .....	13
Configuring ArcSight Manager Logging .....	13

---

Sending logs and diagnostic information to ArcSight .....	14
Guidelines for using the Send Logs utility .....	14
Gathering logs and diagnostic information .....	15
Understanding SSL Authentication .....	20
Terminology .....	20
Tools for SSL configuration .....	25
Keytoolgui .....	25
keytool .....	28
tempca .....	29
How SSL Works .....	29
SSL certificates .....	31
Types .....	31
Comparing Self-signed and CA-signed certificates .....	31
Using a Demo Certificate .....	32
Using a Self-Signed Certificate .....	33
When clients communicate with one ArcSight Manager .....	33
When clients communicate with multiple ArcSight Managers .....	35
Using a CA-Signed Certificate .....	37
Obtaining a CA-signed certificate .....	37
Importing a CA-signed certificate into Manager's key store .....	38
Replacing an Expired Certificate .....	41
Establishing SSL Client Authentication .....	42
Setting up SSL Client Authentication on ArcSight Console running in Default Mode ....	42
Setting up SSL Client Authentication on ArcSight Web running in Default Mode .....	49
Setting up SSL Client Authentication for Console running in FIPS Mode .....	54
Setting up SSL Client Authentication for ArcSight Web running in FIPS Mode .....	55
Migrating from one certificate type to another .....	56
Migrating from Demo to Self-Signed .....	56
Migrating from Demo to CA-Signed .....	56
Migrating from Self-Signed to CA-Signed .....	57
Verifying SSL Certificate Use .....	57
Sample output for verifying SSL certificate use .....	57
Changing the Password for keystore/truststore .....	58
Using Certificates to Authenticate Users to ArcSight .....	59
Using the Certificate Revocation List (CRL) .....	60
Reconfiguring the ArcSight Console after Installation .....	60
Reconfiguring ArcSight Manager .....	61
Changing ArcSight Manager Ports .....	61
Changing ArcSight Web Session Timeouts .....	61
Manager Password Configuration .....	62
Enforcing Good Password Selection .....	62
Password Length .....	62
Restricting Passwords Containing User Name .....	62

---

Requiring Mix of Characters in Passwords .....	62
Checking Passwords with Regular Expressions .....	63
Password Uniqueness .....	64
Setting Password Expiration .....	64
Restricting the Number of Failed Log Ins .....	65
Re-Enabling User Accounts .....	65
Compression and Turbo Modes .....	65
Enabling Compression for ArcSight SmartConnector Events .....	65
Understanding ArcSight Turbo Modes .....	66
Configuring the ArcSight Database Monitor .....	67
Configuring Database Monitor e-mail message recipients .....	67
Configuring the check for free space in Oracle tablespaces .....	67
Sending Events as SNMP Traps .....	68
Configuration of the SNMP trap sender .....	68
<b>Chapter 3: Database Administration .....</b>	<b>71</b>
Changing Oracle Initialization Parameters .....	72
Monitoring Available Free Space in Tablespaces .....	73
Setting Up Database Threshold Notification .....	73
Resetting the Oracle Password .....	73
Speeding up partition compression .....	73
Partition logs .....	74
<b>Chapter 4: Managing Resources .....</b>	<b>75</b>
Managing Users .....	76
Handling Users .....	76
Creating a User .....	76
Editing a User .....	78
Resetting User Passwords .....	78
Moving or Linking a User .....	78
Deleting a User .....	78
About the System User .....	79
Handling User Groups .....	79
Creating User Groups .....	80
Renaming User Groups .....	80
Editing User Groups .....	80
Moving or Linking User Groups .....	80
Deleting User Groups .....	80
Setting Startup Views .....	81
Managing Permissions and Resources .....	81
Editing Access Control Lists (ACLs) .....	81
Granting or Removing Resource Permissions .....	82
Granting or Removing Operations Permissions .....	84

---

Granting or Removing User Group Permissions .....	85
Granting or Removing Event Permissions .....	86
Granting or Removing Sortable Field Sets Permissions .....	88
Sharing Resources .....	89
Controlling Who Has Permissions to Deploy Data Monitors .....	90
How Upgrades Affect Data Monitor Deploy Permissions .....	91
Deployment Permissions on Imported Data Monitors .....	92
Locking and Unlocking Resources .....	92
System Core Content .....	92
User Created Content .....	92
Unlocking a User-locked Resource .....	93
Modeling Your Network and Managing Assets .....	93
Network Model .....	93
Populating the Network Model with Assets .....	94
Understanding ESM Asset Resources .....	95
Assets .....	95
Locations .....	95
Zones .....	95
Networks .....	96
Vulnerabilities .....	96
Asset Categories .....	96
Populating the Network Model Using the Wizard .....	97
Specifying CSV Column Types .....	97
Zones CSV File Format .....	100
Assets CSV File Format .....	101
Asset Ranges CSV File Format .....	103
Increasing the Number of Rows Displayed .....	104
Summary of Data to Import .....	105
Network Data Imported into Manager .....	105
Selecting Assets in the Common Conditions Editor .....	107
Managing Assets .....	107
Creating an Asset .....	108
Working with Locations, Zones, Networks, Vulnerabilities, and Categories .....	108
Editing an Asset .....	111
Moving or Copying an Asset .....	111
Deleting an Asset .....	111
Showing Assets in a Channel .....	111
Auto Zoning an Asset .....	112
Managing Asset Groups .....	112
Creating an Asset Group .....	112
Renaming an Asset Group .....	112
Editing an Asset Group .....	112
Moving or Copying an Asset Group .....	113

---

Deleting an Asset Group .....	113
Asset Scalability .....	113
Viewing Assets in Active Channels .....	113
Finding Assets .....	113
Selecting Vulnerabilities .....	113
Managing Vulnerabilities .....	114
Creating a Vulnerability .....	114
Editing a Vulnerability .....	115
Moving or Copying a Vulnerability .....	115
Retrieving Vulnerable Assets .....	115
Adding an Asset to a Vulnerability .....	116
Deleting an Asset From a Vulnerability .....	116
Deleting a Vulnerability .....	116
Managing Vulnerability Groups .....	116
Creating a Vulnerability Group .....	116
Renaming a Vulnerability Group .....	116
Editing a Vulnerability Group .....	116
Moving or Copying a Vulnerability Group .....	117
Deleting a Vulnerability Group .....	117
Reporting on Scanners .....	117
Reporting Vulnerable Assets .....	117
Managing Filters .....	118
Using Filters .....	118
Editing a Filter .....	118
Importing and Exporting filters .....	119
Moving or Copying Filters .....	119
Deleting Filters .....	119
Using Filter Groups .....	119
Creating Filter Groups .....	119
Renaming Filter Groups .....	119
Editing Filter Groups .....	120
Moving or Copying Filter Groups .....	120
Deleting Filter Groups .....	120
Managing Notifications .....	120
Managing Received Notifications .....	120
Managing Notification Groups and Levels .....	121
Creating Notification Groups .....	121
Renaming Notification Groups .....	122
Editing Notification Groups .....	122
Deleting Notification Groups .....	122
Adding Escalation Levels .....	122
Deleting Escalation Levels .....	122
Managing Notification Destinations .....	122

---

Creating Destinations .....	122
Editing Destinations .....	123
Moving or Copying Destinations .....	123
Deleting Destinations .....	123
Changing Notification and Acknowledgement Settings .....	123
Changing E-mail Settings .....	124
Adding New Pager Service Providers .....	124
Editing Pager Service Provider Settings .....	125
Deleting Pager Service Providers .....	125
Changing Wait Time Settings .....	125
Testing Notification Groups and Destinations .....	125
Testing Group Notifications .....	125
Testing Destination Notifications .....	125
Managing File Resources .....	126
Uploading Files and Creating a File Resource .....	126
Viewing Files .....	128
Downloading Files Locally .....	128
Editing File Resource Attributes .....	128
Replacing File Resource Contents .....	128
Deleting File Resources .....	128
Adding a File or Folder to a Package .....	128
Finding Files .....	129
Managing Packages .....	129
Viewing Installed Packages .....	130
Viewing all Packages (with Dependencies) .....	130
Showing Package Archive Contents .....	130
Creating Packages .....	130
Importing Bundles .....	132
Exporting Packages .....	133
Installing Packages .....	133
Uninstalling Packages .....	133
Editing Packages .....	134
Adding Resources to Packages .....	134
Removing Resources from Packages .....	134
Deleting Packages .....	134
Resolving Package Conflicts .....	135
Managing SmartConnectors .....	136
Selecting and Setting SmartConnector Parameters .....	136
Configuring the SmartConnector .....	136
Connector Editor Option Tabs .....	136
Connector Tab Configuration Fields .....	137
Default Content Tab Configuration Fields .....	139
SmartConnector Processing Categories .....	151



---

SmartConnector Time Interval Options .....	152
Managing SmartConnector Filter Conditions .....	152
Creating SmartConnector Filters .....	152
Adding SmartConnector Filter Conditions .....	153
Deleting SmartConnector Filter Conditions .....	153
Setting Special Severity Levels .....	153
Setting a Custom Severity Level .....	153
Configuring a Conditional Severity .....	154
Sending Model Mappings to SmartConnectors .....	154
Sending Model Mappings to a Connector .....	154
Sending Control Commands to SmartConnectors .....	154
Getting Status Reports .....	155
Sending Flow-Control Commands .....	155
Managing SmartConnector Groups .....	162
Creating SmartConnector Groups .....	163
Renaming SmartConnector Groups .....	163
Editing SmartConnector Groups .....	163
Moving or Copying SmartConnector Groups .....	163
Deleting SmartConnector Groups .....	163
Managing SmartConnector Resources .....	163
Moving or Copying a SmartConnector Group .....	163
Deleting a SmartConnector Group .....	164
Importing and Exporting SmartConnector Configurations .....	164
Importing a SmartConnector Configuration .....	164
Exporting a SmartConnector Configuration .....	165
SmartConnector Filters .....	166
Upgrading SmartConnectors .....	166
Overview of the Upgrade Process .....	166
Upgrading SmartConnectors .....	168
Rolling back to a Previous Version .....	169
Troubleshooting .....	169
Selecting Resources .....	170
Finding Resources .....	171
Searching for System Resources .....	171
Search Field on Console Tool Bar .....	171
Query Options .....	172
Result Columns .....	173
Locating Specific Resources .....	173
Visualizing Resources .....	174
Graphing Resources .....	174
Using Graphs .....	174
Configuring Resource Graphs .....	176
Viewing Resources in Grids .....	177

---

Validating Resources .....	177
Valid and Invalid Resources .....	178
Fixing and Validating Resources .....	178
Troubleshooting (Requirements for Valid Resources) .....	180
Automatic and Manual Validation .....	183
Resource Validation During Upgrade .....	183
Extending Audit Event Logging .....	184
Managing Partitions .....	184
Getting Partition Information .....	185
Seeing a Partition Schedule .....	185
Archiving Partitions .....	185
Reactivating Archived Partitions .....	186
Reactivating Zipped or Large Archived Partitions .....	186
Deactivating Archived Partitions .....	187
Running Scheduled Tasks Right Away .....	187
Partition Properties .....	187
Managing Customers .....	188
Creating Customers .....	188
Editing Customers .....	188
Deleting Customers .....	188
Saving Copies of Read-Only Resources .....	189
Using the Image Editor .....	189
Common Resource Attribute Fields .....	189
Common .....	189
Assign .....	190
Parent Groups .....	190
Creation Information .....	190
Last Update Information .....	191
<b>Appendix A: ArcSight Commands .....</b>	<b>193</b>
Running an ArcSight Command Script .....	193
Categorized ArcSight Commands .....	193
Alphabetic List of Commands .....	196
<b>Appendix B: Troubleshooting .....</b>	<b>239</b>
General .....	239
Query and Trend Performance Tuning .....	242
Regenerate Event Statistics .....	242
Persistent Database Hints .....	242
server.defaults.properties Entries for Trends .....	242
Troubleshooting Checklist after Restarting the Manager .....	243
Reports for Monitoring Trend Performance .....	243
Disable these Trends on High Throughput Systems .....	243

---

How will you know when a trend is caught up? .....	244
How long will it take a trend to catch up? .....	244
Enhancing the Performance Globally for all Database Queries .....	244
SmartConnectors .....	245
Console .....	246
Manager .....	247
ArcSight Web .....	248
Database .....	249
SSL .....	250
<b>Appendix C: Monitoring Database Attributes .....</b>	<b>253</b>
Understanding Database Checks .....	253
Message text .....	253
Disabling Database Checks .....	255
List of Database Check Tasks .....	255
<b>Appendix D: The Logfu Utility .....</b>	<b>257</b>
Running Logfu .....	257
Example .....	259
Troubleshooting .....	259
Menu .....	261
Typical Data Attributes .....	261
Intervals .....	263
<b>Appendix E: Creating Custom E-mails Using Velocity Templates .....</b>	<b>265</b>
Overview .....	265
Notification Velocity templates .....	265
Commonly used elements in Email.vm and Informative.vm files .....	265
The #if statement .....	265
Contents of Email.vm and Informative.vm .....	266
How the Email.vm and Informative.vm Template Files Work .....	267
Understanding the Customization Process .....	267
Customizing the template files .....	268
Sample Output .....	268
<b>Appendix F: The Archive Command Tool .....</b>	<b>271</b>
Overview of the Archive Command Tool .....	271
Exporting Resources to an Archive .....	272
Importing Resources from an Archive .....	273
About Importing v3.x Content to a v4.x ESM System .....	273
Syntax for Performing Common Archive Tasks .....	276
<b>Appendix G: Advanced Configuration to Support Standard Content .....</b>	<b>279</b>
Configure SmartConnectors to Send Connector Device Status Events for Critical Devices .....	279

---

Configure Connector Up/Down Resources .....	280
Configure Critical Device Not Reporting Resources .....	281
Configure White List Filters .....	282
Configure Critical Device Not Reporting Rule .....	284
<b>Index .....</b>	<b>285</b>

# About this Guide

---

[“Related Documentation” on page xiii](#)

[“Feedback” on page xvi](#)

This section describes the purpose of the ArcSight Administrator’s Guide. It also lists other documents available for ArcSight ESM and briefly describes the information contained in those documents.

The ArcSight Administrator’s Guide provides you information about configuring and running your ArcSight ESM system. This guide assumes that you have successfully installed your ArcSight ESM system.

Information about ArcSight ESM system components, supported platforms, deployment scenarios, and how to install the components is covered in the ArcSight Installation and Configuration Guide.

## Related Documentation

The complete ArcSight documentation set includes guides and Online Help listed in the following table. All guides are available in PDF format.

You can access the guides in these ways:

- From the ArcSight Manager doc directory.
- From the ArcSight Customer Support web site at <https://support.arcsight.com>.
- From the ArcSight Console online Help (click **Help | Browse Arcsight Documentation**).

You can access the ArcSight ESM Online Help from the Help option in ArcSight Console (click **Help | Help Contents**).

Document Title	Description
ESM 101: Concepts for ArcSight™ ESM	ESM 101 introduces the underlying concepts behind how ArcSight ESM works, and provides a roadmap to the tools available in ESM depending on your role in security operations.
ArcSight™ ESM Release Notes	Describes new product features, latest updates, known product issues and work-arounds, and technical support information.

Document Title	Description
ArcSight™ ESM Installation and Configuration Guide	Explains how to install and configure ArcSight Enterprise Security Management (ESM) components and tools including the ArcSight Database, Manager, Console, and Web applications. Also provides general information about how to plan for, install, and deploy ArcSight SmartConnectors.
ArcSight™ ESM Administrator's Guide	Describes how to configure ArcSight and its network interfaces, and maintain ArcSight for ongoing operations.
ArcSight™ ESM Reviewer's Guide	Introduces major new features in the current version of ArcSight ESM, including task walk-throughs and usage guidance. The same information is highlighted in the "What's New" Console Help topics.
ArcSight™ ESM User's Guide ArcSight™ ESM Reference Guide	Describes how to use the ArcSight Console. These are printable versions of the online Help topics and glossary.
ArcSight™ ESM Web User's Guide	Provides user and reference information from the ArcSight Web online Help system.
ArcSight™ SmartConnector Configuration Guides	Provides vendor-specific instructions for how to install individual SmartConnectors and configure their associated devices.
ArcSight FlexConnector Configuration Guide	Describes how to design, create, and install custom SmartConnectors.

## Notes, Tips, and Cautions



Represents a Note.

Notes provide additional information about a feature or procedure that might help the user make decisions, or inform users about outcomes they can expect.



Represents a Tip.

Tips provide helpful suggestions and best practices about how to get optimum results from a feature or procedure.



Represents a Caution.

Cautions provide information that when ignored may cause system damage, data loss, or bodily injury.

## Text Conventions

The following table lists the syntax conventions used in this guide.

Text	Description and Example
<b>Bold</b>	<p>Bold is used to indicate an on-screen element that a user should click. Always use this character format rather than manually bolding the item with the format   style menu or "bold" button.</p> <ul style="list-style-type: none"> <li>Enter a value and click <b>OK</b>.</li> </ul>
<code>Code</code>	<p>As described before, the code character tag is used for code elements discussed in-line in a paragraph.</p> <ul style="list-style-type: none"> <li>If the name of your active list entries text file is <code>"AdministrativeUsers.txt"</code>, the script would look like this:</li> </ul>
<i>Emphasis or BookName</i>	<p><i>Italics</i> indicates emphasis or a book name:</p> <ul style="list-style-type: none"> <li><i>Do not</i> perform this procedure until you have backed up your data.</li> <li>For more information, see the <i>ArcSight Administrator's Guide</i>.</li> </ul>
<b>menu &gt; submenu</b>	<p>Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences.</p> <ul style="list-style-type: none"> <li><b>menu &gt; submenu &gt; submenu</b></li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li><b>Authoring &gt; Rules &gt; Rule Actions &gt; Updating Session Lists</b></li> </ul>
tab   subtab	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none"> <li>tab   subtab   subtab</li> </ul>
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none"> <li>All Reports/System Reports/Asset/All Assets</li> </ul>
<variable>	<p>A text string enclosed in angular brackets is a variable for which you need to supply a value. (The bracketed text may also be in italics to emphasize that it is a variable.)</p> <p>Example:</p> <p>In <code>--nsp_password=&lt;password&gt;</code>, <code>&lt;password&gt;</code> is a variable for which you supply a value.</p>
{parameter1   parameter2   parameter3}	<p>Curly brackets enclose multiple parameters, at least one of which you must provide.</p> <p>Example:</p> <pre>{--user_id_seq=&lt;user_id&gt;   -- user_login=&lt;user_login&gt;}</pre> <p>In the above example, either supply the user ID of a user or his/her login name.</p>
[optional_parameter]	<p>Square brackets enclose parameters, variables, or values that are optional.</p> <p>Example:</p> <pre>[--cli_restrict=1]</pre>

## Feedback

To submit feedback regarding ArcSight ESM or documentation, go to ArcSight's customer support web site at <https://support.arcsight.com>



# 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 ArcSight Database.

The following topics are covered here:

- ["Running ArcSight ESM" on page 2](#)
- ["Starting the ArcSight Manager" on page 2](#)
- ["Starting the ArcSight Console" on page 3](#)
- ["Starting ArcSight SmartConnectors" on page 3](#)
- ["Stopping the ArcSight Manager" on page 4](#)
- ["Reconnecting to the ArcSight Manager" on page 4](#)
- ["Configuring ArcSight Manager or ArcSight Web as a Service" on page 4](#)
- ["Reducing Impact of Anti-Virus Scanning" on page 6](#)

## 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 up 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 `<ARCSIGHT_HOME>/bin` directory:
- 3 Type in the following line and press Enter.

```
arcsight manager
```

When you start up, 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`. For example, on Unix systems, you could 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 terminal box 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 login message as well, provided that the browser used supports JavaScript and has JavaScript enabled.

## 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 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 command window 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.



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, ArcSight recommends 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`

## Chapter 2

# Configuration

---

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

- [“Managing and Changing Properties File Settings” on page 8](#)
- [“Adjusting Console Memory” on page 12](#)
- [“Installing New License Files Obtained from ArcSight” on page 13](#)
- [“Configuring ArcSight Manager Logging” on page 13](#)
- [“Understanding SSL Authentication” on page 20](#)
- [“Reconfiguring the ArcSight Console after Installation” on page 60](#)
- [“Reconfiguring ArcSight Manager” on page 61](#)
- [“Manager Password Configuration” on page 62](#)
- [“Compression and Turbo Modes” on page 65](#)
- [“Configuring the ArcSight Database Monitor” on page 67](#)
- [“Sending Events as SNMP Traps” on page 68](#)

## Managing and Changing Properties File Settings

Various components of ArcSight 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 ESM 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 in ArcSight ESM.

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
TCP	1521	ArcSight Manager to ArcSight Database (Oracle communication)
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, 2006, 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.2006_09_27_14_45_27_718
```

On September 28, 2006, 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.2006_09_27_14_45_27_718
```

```
server.properties.2006_09_28_01_05_40_615
```

On September 29, 2006, 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.2006_09_27_14_45_27_718
```

```
server.properties.2006_09_28_01_05_40_615
```

```
server.properties.2006_09_29_03_25_45_312
```

On September 30, 2006, 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.2006_09_27_14_45_27_718
```

```
server.properties.2006_09_28_01_05_40_615
```

```
server.properties.2006_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 193](#).

- 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.



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.

---

## 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.



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.

## 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:

```
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.

## 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/server.log
```

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, compresses them, and (optionally) uploads them to the ArcSight Customer Support server.

Starting with version 4.0, this utility has been enhanced as follows:

- 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.



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 193](#).

- When you run this utility from the Console, Manager, or ArcSight Web, you can gather logs and diagnostic information for all components of the ArcSight 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 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 `arcdbt` command on the Manager. For more information, see [Appendix A, ArcSight Commands, on page 193](#).
- 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 compressed file is uploaded to the ArcSight Customer Support server using SSL. Therefore, you must have one of the following to allow your ArcSight component to make SSL connections to the ArcSight Customer Support server:
  - ◆ Port 443 open on your firewall
  - ◆ A proxy server that the ArcSight component can use
- Automatic upload of the compressed file is optional. If you do not choose to upload automatically, 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 before it is uploaded 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`:

```
arc sight agent sendlogs
```

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

- On the ArcSight Console, click **Tools | SendLogs**.

- Enter this command in `<ARCSIGHT_HOME>/bin` on Console, Manager, or ArcSight Web:

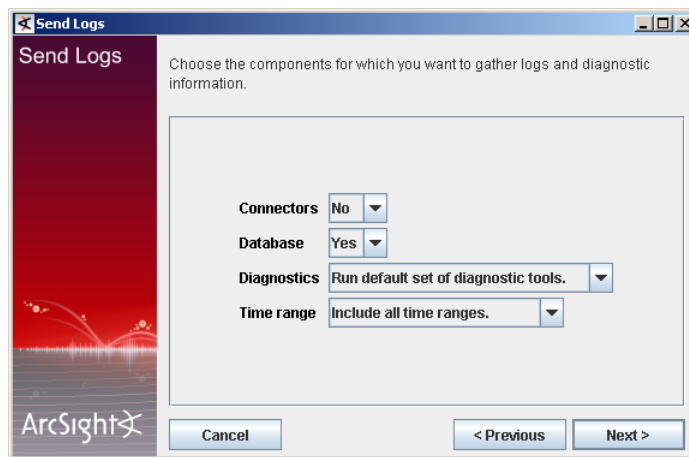
```
arcsight sendlogs
```

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



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 ESM components.
- 2 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. Note that the file must contain only one SQL command; multiple SQL commands are not allowed.

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
```

Do not end the SQL command in the above example with a semi-colon (;).

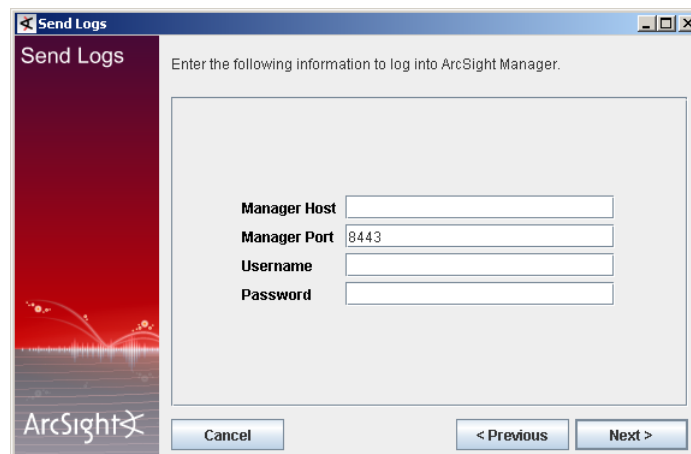
- ii Run this command:

```
arcdt runsql temp/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.

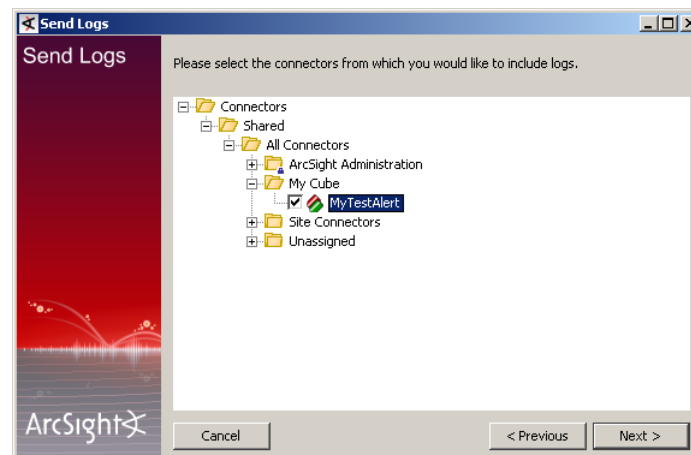


- 3 Enter information to log in to your ArcSight Manager.



The 'Send Logs' dialog box has a title bar with standard window controls. The left sidebar features the ArcSight logo and a red background with a stylized fire graphic. The main area contains the text 'Enter the following information to log into ArcSight Manager.' Below this are four input fields: 'Manager Host' (empty), 'Manager Port' (containing '8443'), 'Username' (empty), and 'Password' (empty). At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

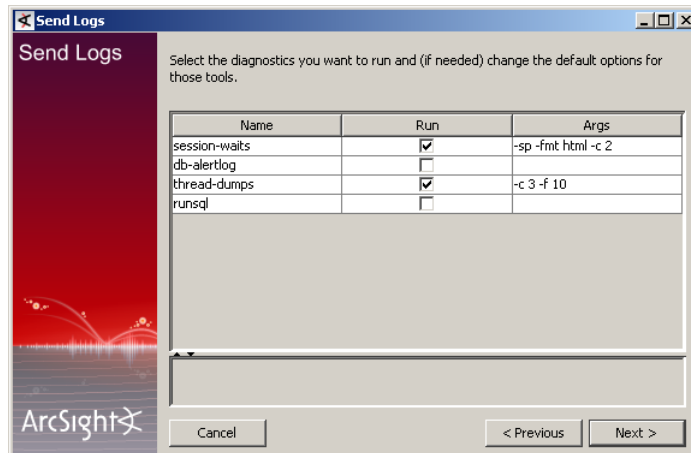


The 'Send Logs' dialog box shows a tree view of connectors. The left sidebar is identical to the previous screen. The main area contains the text 'Please select the connectors from which you would like to include logs.' The tree view shows a hierarchy: 'Connectors' (expanded) -> 'Shared' (expanded) -> 'All Connectors' (expanded) -> 'ArcSight Administration' (expanded) -> 'My Cube' (expanded) -> 'MyTestAlert' (checked). Other connectors like 'Site Connectors' and 'Unassigned' are also listed. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

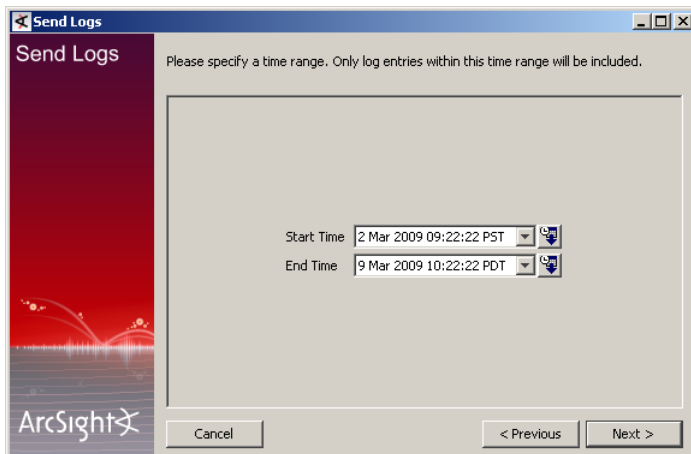


At a minimum, the SmartConnectors should be running version 4037 or later.

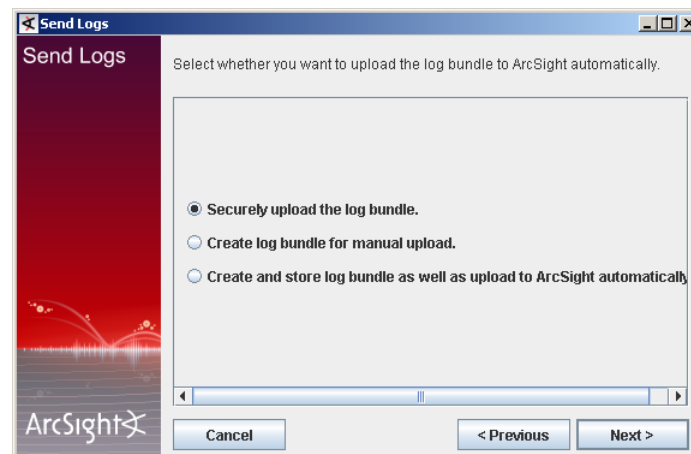
- 5 If you chose to select the diagnostic utilities you want to run earlier in this wizard, select them in the next screen.



- 6 If you chose to specify a time range for which the wizard will gather the logs, specify it in the next screen.



- 7 Select from various upload options available as shown in the next screen.



- 8 Select whether a proxy server is required to connect to the external web from the component on which you are running the wizard.

If a proxy server is required, enter that information, in the next screen.

The 'Send Logs' dialog box has a title bar with standard window controls. The main area contains the text 'Enter information about the proxy server.' and a note: 'Note: If you do not use proxy authentication, please leave the Username and Password fields empty.' Below this are five input fields: 'Proxy Host', 'Proxy Port', 'Use Authentication' (a dropdown menu currently set to 'No'), 'Username', and 'Password'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 9 Enter the information for the ArcSight Customer Support server to which the `sendlogs` command uploads the compressed logs and diagnostic information.

The 'Send Logs' dialog box has a title bar with standard window controls. The main area contains the text 'Enter your user name (e-mail address) and password for the ArcSight Customer Support upload server (software.arcsight.com).' Below this are three input fields: 'E-Mail', 'Password', and 'Save Password' (a dropdown menu currently set to 'No'). At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.



Use the e-mail address and password that you use to log in to ArcSight Customer Support's web site, <https://software.arcsight.com>. If you do not have this information, contact ArcSight Customer Support.

- 10 Select whether you want to review the compressed log file information before uploading that file to the ArcSight Customer Support site.
- 11 Select whether you want to sanitize the logs before sending. For more information about sanitizing options, see Guidelines for using the `sendlogs` utility.

If you choose to remove IP addresses, host names, and e-mail addresses, enter the host name suffixes for which host names and e-mail addresses should be removed.

- 12 Enter the incident number.

The `sendlogs` 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.

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

- 13** Click **Next** to start the compression and, if you previously chose to do so, the automatic upload process.



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 such as the incident number and password for uploading logs to ArcSight Customer Support.

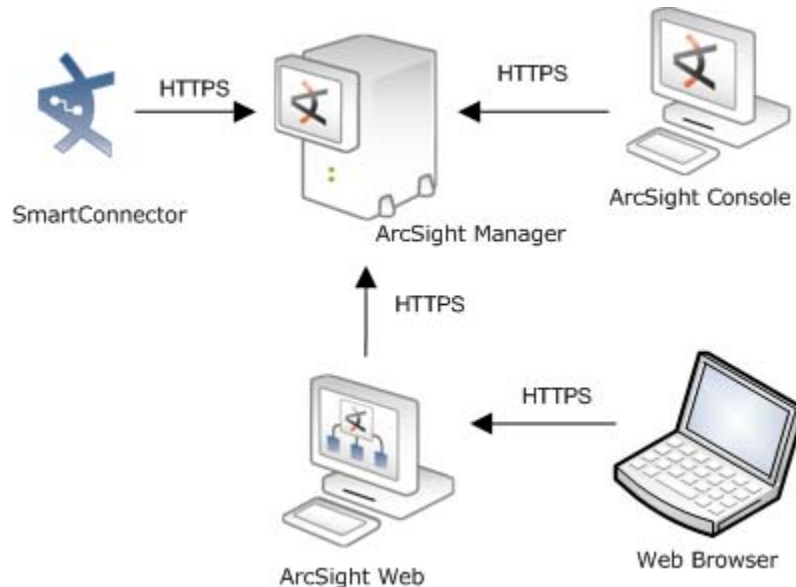
## Understanding SSL Authentication

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 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 29](#).



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 25](#).

### ■ 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.

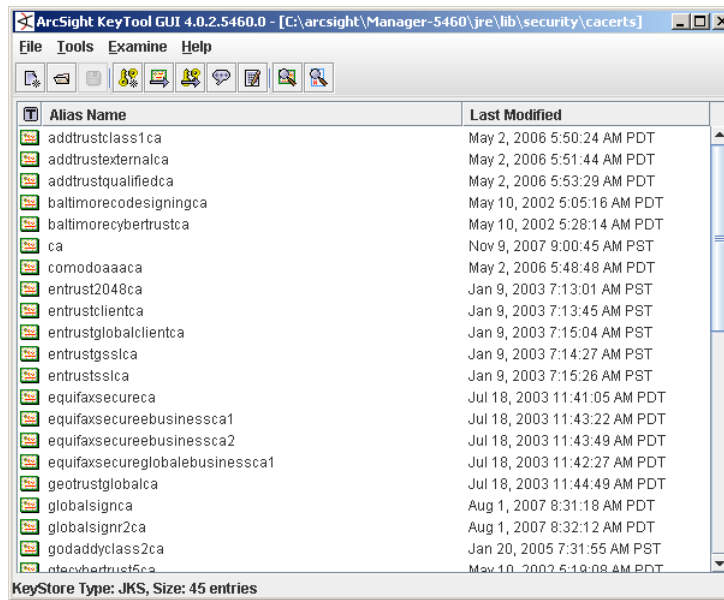
### ■ Key store

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	<code>keystore</code>	<code>&lt;ARCSIGHT_HOME&gt;/config/jetty</code>
ArcSight Web	<code>webkeystore</code>	<code>&lt;ARCSIGHT_HOME&gt;/config/jetty</code>
Clients* (for client-side authentication)	<code>keystore.client</code>	<code>&lt;ARCSIGHT_HOME&gt;/config</code>

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

### 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 25.

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 29.

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

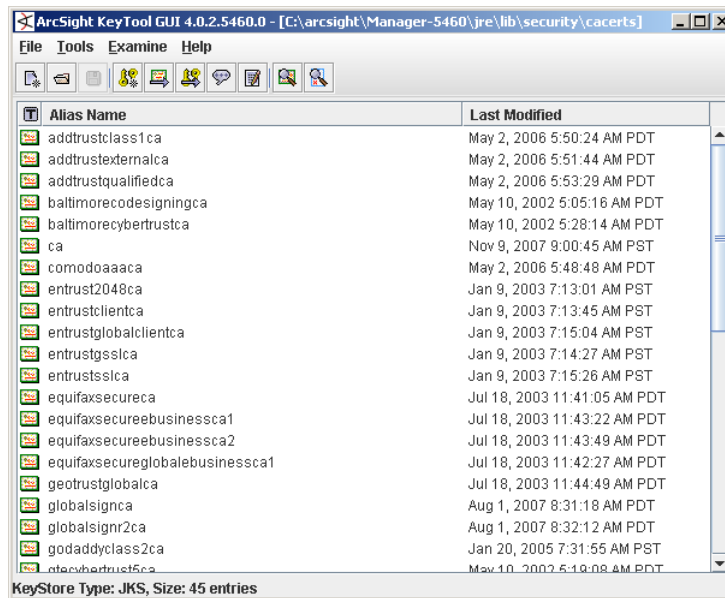
Component	Trust Store File Name	Location of Trust Store
Clients	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	cacerts[1]	<ARCSIGHT_HOME>/jre/lib/security
ArcSight Web	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	truststore[2]	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webtruststore[2][3]	<ARCSIGHT_HOME>/config/jetty

[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. For example, in the following trust store, [techpubs.arcsight.com](http://techpubs.arcsight.com) is an alias for a certificate created for the machine [techpubs.arcsight.com](http://techpubs.arcsight.com).

## ■ 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>

Password Type	Property File	Property Name
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.

In v3.5 and later, 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)
- Importing a certificate
- Viewing a key store

The `keytoolgui` utility is available on all components of ArcSight ESM in the `<ARCSIGHT_HOME>/bin/scripts` directory.



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:

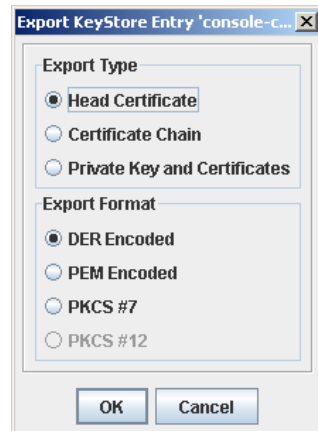
```
arcsight agent keytoolgui
```

### Using Keytoolgui to Export a Certificate

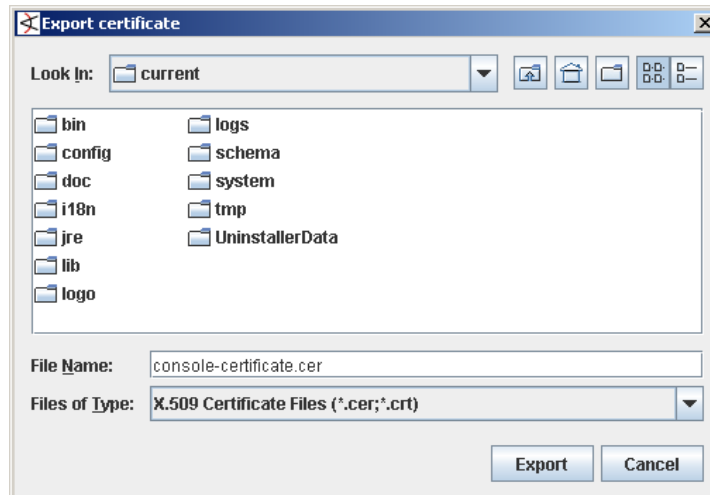
- 1 Start the `keytoolgui` from the component from which you want to export the certificate. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory.
 

```
arcsight keytoolgui
```
- 2 Select **File->Open KeyStore** and navigate to your truststore.
- 3 Enter the truststore password when prompted. The default password is “changeit” without the quotes.
- 4 Right-click the certificate and select **Export**.

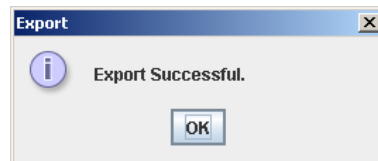
- a Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- b 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**.



- c You will see the following message:



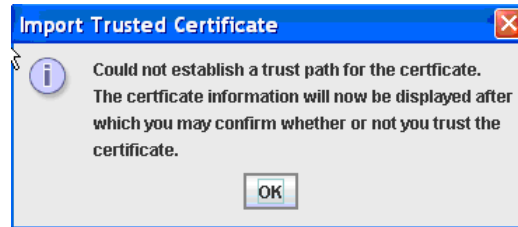
- 5 If the component into which you want to import this certificate resides on a different machine than the machine from which you exported the certificate (the current machine), copy this certificate to the other machine.

### Using Keytoolgui to Import a Trusted Certificate

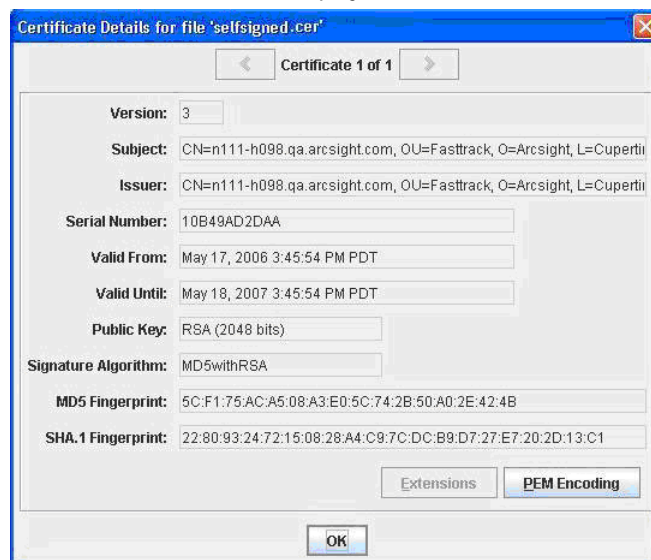
- 1 Start the keytoolgui from the component into which you want to import the certificate. To do so, run the following command from the component's `<ARCSIGHT_HOME>/bin` directory.

```
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`.
- 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**.

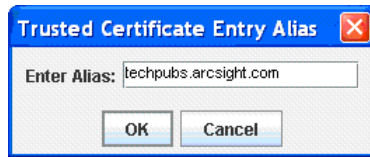


- 9 You will see the following message. Click **OK**.



- 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 Keypair 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 keypair 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 [options] -store store
```

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

On SmartConnector hosts, use:

```
arcsight agent keytool [options] -store store
```

To see options available for each store, enter:

```
arcsight keytool -store store
```



There are 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
```

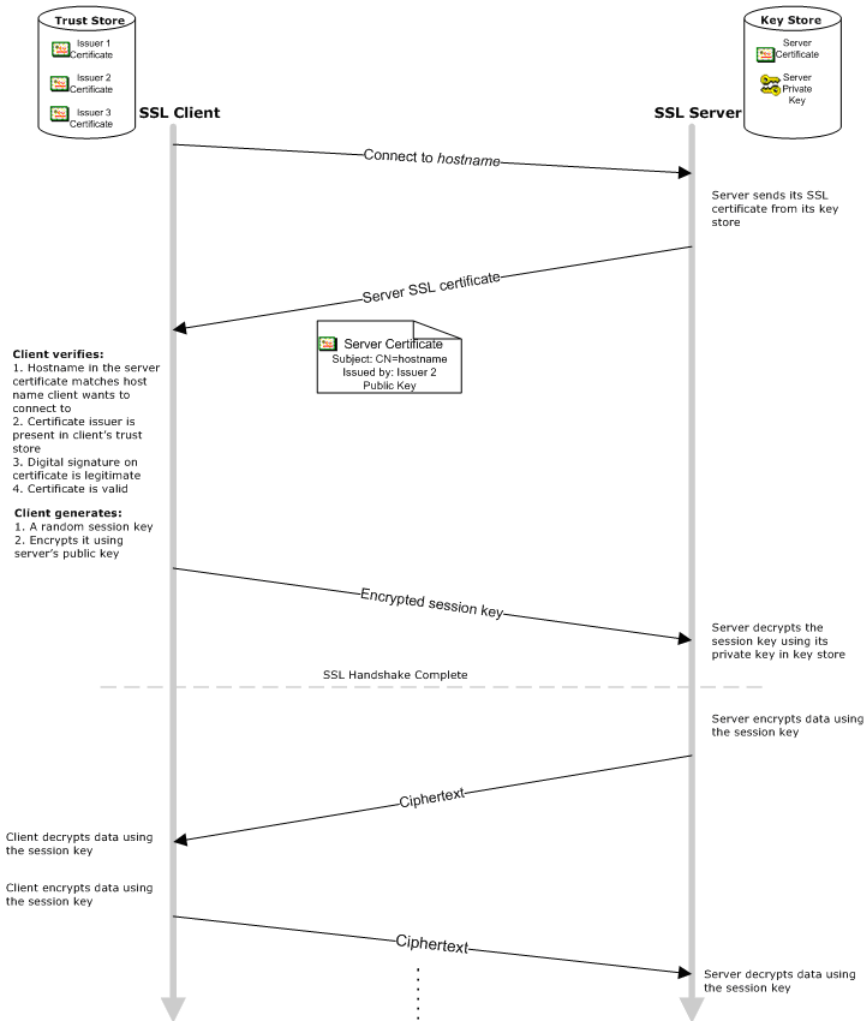
## How SSL Works

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



To replace an expired certificate, you have to delete the old expired certificate from the truststore, cacerts (in the case of default mode) or nssdb (in the case of FIPS mode), first and then import the new certificate into cacerts or nssdb. 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 or nssdb.

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**. To delete the certificate from the nssdb, run the following command from the ArcSight component's `bin` directory:

```
arcsight runcertutil -D -n <certificatename> -d <nssdbdir>
```

Use the keytoolgui to import the new certificate into the truststore or cacerts. See the *ArcSight ESM Installation and Configuration Guide* for details on how to import a certificate into the nssdb.



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 for ArcSight ESM:

- 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 37](#).

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`:  

```
runconsolesetup
```
  - 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`:  

```
runwebsetup
```
  - 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:

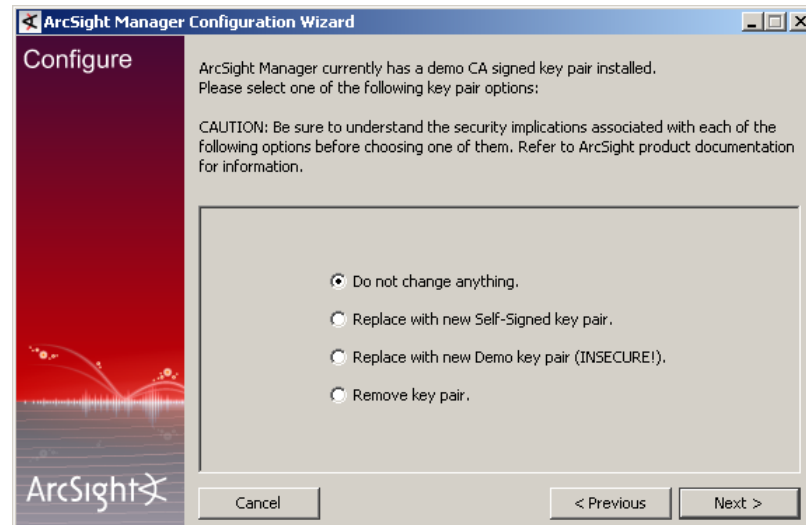


Steps to create a self-signed key pair may be different for a new ArcSight Manager installation as the Configuration Wizard is launched automatically during the installation process.

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

```
arcsight managersetup
```

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



- 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 `self-signed.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`.



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

- 2 Copy the cacerts file from the Manager to the `<ARCSIGHT_HOME>/jre/lib/security` directory on all clients.



This step overwrites your existing cacerts file 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.



Make sure you have copied the cacerts file to all existing clients before proceeding further. Otherwise, after you perform the next steps, only clients with the new cacerts file will be able to connect to the Manager.

- 3 Restart the Manager process so that the Manager can start using the self-signed certificate.
- 4 Restart all clients.
- 5 When installing a new client, repeat Step 2 of this procedure.
- 6 On the ArcSight Web server, perform the steps listed in section [“Setting up SSL Client Authentication on ArcSight Web running in Default Mode”](#) on page 49

## 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:



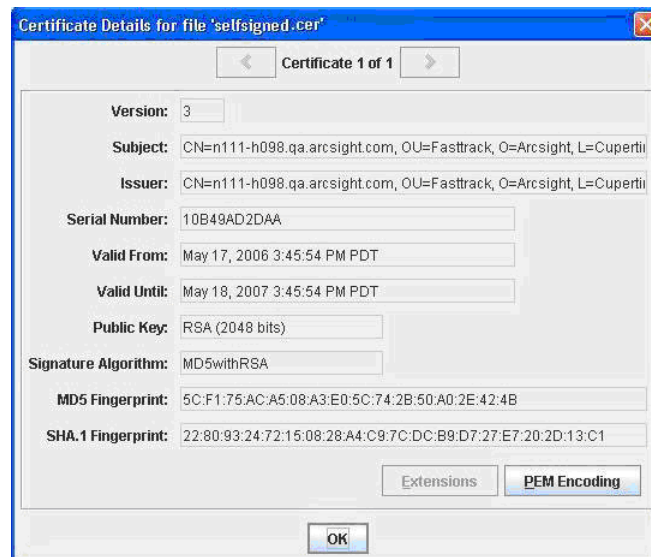
By following this procedure you append the self-signed certificate to the existing client trust store, cacerts. Doing so prevents overwriting cacerts, which happens if you follow the previous procedure.

- 1 Follow Step 1 from the previous procedure on all Managers.
- 2 Copy the self-signed.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**.

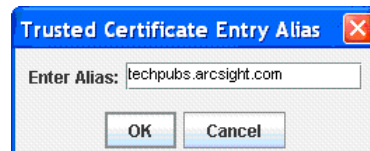


- iii You will see the following message. Click **OK**.



- 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.



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.  
Select from these key store types:
    - 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**.



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 (a name for referring to the new key pair in the future).



The default alias is the Common Name (CN) you provided in the previous step. However, it is mandatory that you change the name to mykey.

- 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.

- 3 Send the CSR to the selected Certificate Authority (CA).

After verifying the information you send, the CA electronically signs the certificate using its private key and replies with a certification response that contains the signed certificate.

## Importing a CA-signed certificate into Manager's key store

When the CA has processed your request, it sends you a file with the signed certificate.

The SSL certificate you receive from the Certificate Authority must be a 128-bit X.509 Version 3 certificate. The type of certificate is the same one that is used for common web servers. The signed certificate must be returned by the CA in base64 encoded format. It will look similar to this:

```
-----BEGIN CERTIFICATE-----
MIICjTCCAfagAwIBAgIDWnWvMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQT
EiMCAGA1UECBMZRk9SIFRlRjRkcgUFRVSVUE9TRVMgT05MWTEdMBsGA1UEChMUUVGhh
d3RlIENlcnRpZmljYXRpb24xZzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQ
QDExNUaGF3dGUgVGVzdCBDQSBsb290MB4XDTAyMDkyNzIzMzI0MVoxDTAyMTAxODIZ
MzI0MVowaDELMAkGA1UEBhMCrVMxDTALBgNVBAGTBGJsYWgxDTALBgNVBAcTBGJsYW
gxDTALBgNVBAoTBGJsYWgxDTALBgNVBAsTBGJsYWgxHTAbBgNVBAMTFHppZXIuc3Yu
YXJjc2lnaHQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b
+BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vwN4JViC

CSBkDpiqVF7K1lSx4ZVSXX4+VQ6k4gT5G0kDNvQeN05wWkzEMygMB+ZBnYqPA/XtWR
ZtjxvH

MoqS+JEqHruiMLITC6q0reUB/txby6+S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHS
UEDDAKBggrBgEFBQcDATAMBgNVHRMBAg8EAJAAMA0GCSqGSIb3DQEBAUAA4GBAFY3
7E60+P4b3zTLNaG7EVM57GtKED6PwCIi1B6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQV
QxnpABjzTalRfYgjNFJ6ltI6ZKjBO5kim9UBeCnKiNNzhIyDyFwbHXOPB/JaLiV+jG
ugYNS7hf/ay0BXKlfue007EgjjhB/mQFs2JB

-----END CERTIFICATE-----
```

This file must be imported into the key store.

Before proceeding with the following procedure, make sure the issuer that signed your certificate exists as a Trusted CA in cacerts. (Use [keytoolgui](#) to check your cacerts.) If the issuer does not exist, import the root certificate of the CA in the cacerts trust store before importing it in Manager's key store. If the certificate is a chain, you must also import all intermediate certificates.

Follow these steps to import the signed certificate:

- 1 Copy the signed certificate on the Manager in the `<ARCSIGHT_HOME>/config/jetty` directory.
- 2 On the Manager machine, run this command in `<ARCSIGHT_HOME>/bin`:  
`arcsight keytoolgui`
- 3 Click **File->Open Keystore** and select the key store (**keystore.request** or **webkeystore.request**) you saved in [Step f](#) in "Obtaining a CA-signed certificate" on [page 37](#). You will need to provide the password you used to save the key store in that step.
- 4 Right-click the key pair you created at the beginning of the process and named mykey.
- 5 Select **Import CA Reply** from the menu.
- 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):



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:

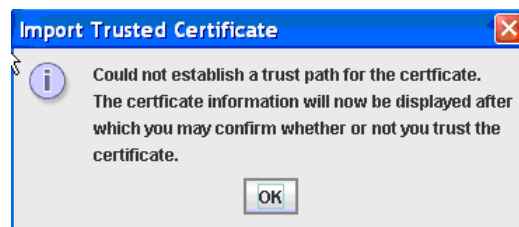
```
arcsight keytoolgui
```

- ii Click **File->Open Keystore**.

- iii Select the store named cacerts. Use the password `changeit` to open cacerts.

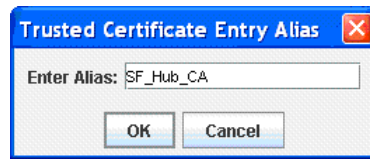
- iv Click **Tools->Import Trusted Certificate** and select the certificate you copied in Step 10a of this procedure.

- 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 key 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.



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/nssdb expires, you need to replace it with a new one. To replace the certificate:

### Default mode:

- 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 32](#), [“Using a Self-Signed Certificate” on page 33](#), or [“Using a CA-Signed Certificate” on page 37](#) section (depending on the type of certificate you are importing) for steps on how to import the certificate.

### FIPS mode:



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.

- 1 Delete the expired certificate from the nssdb. To delete the certificate from the nssdb, run the following command from the ArcSight component's `bin` directory:

```
arcsight runcertutil -D -n <certificate-alias> -d <absolute-path-to-nssdbdir>
```

- 2 Replace the certificate by importing the new certificate into the nssdb. See the *ArcSight ESM Installation and Configuration Guide* for details on how to import a certificate into the nssdb.

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, or nssdb.

## Establishing SSL Client Authentication

By default, clients (SmartConnectors, Consoles, and ArcSight Web) authenticate using user name and password. ESM 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.



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 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:

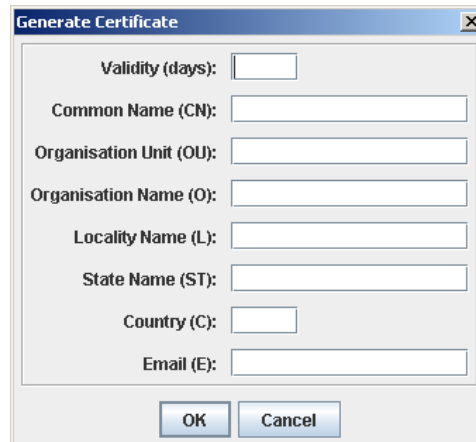
- 1 On each Console, generate a key pair. For CA-signed certificate follow the steps in section [“Obtaining a CA-signed certificate” on page 37.](#):
  - a From the Console's `<ARCSIGHT_HOME>/bin` directory start the keytoolgui by running the following command:

```
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:



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

- 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 keypair in the following dialog and click **OK**:



The 'Key Pair Entry Alias' dialog box contains the following field:

- Enter Alias:


Buttons: OK, Cancel



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 keypair 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**.

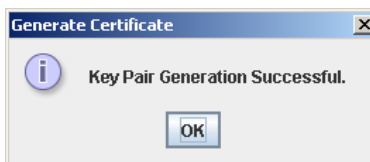


The 'Key Pair Entry Password' dialog box contains the following fields:

- Enter New Password:
- Confirm New Password:

Buttons: OK, Cancel

- g** You will see the following message.



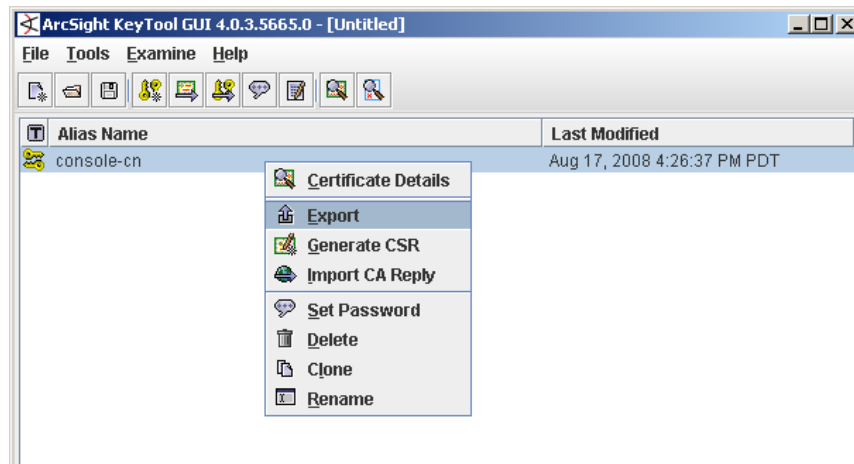
The 'Generate Certificate' dialog box displays the following message:

- Key Pair Generation Successful.

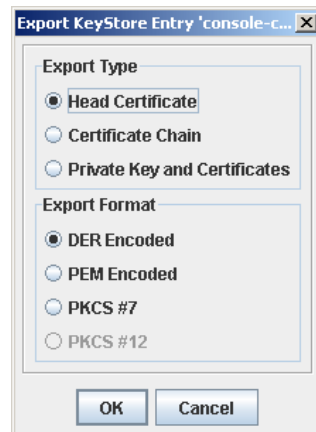
Button: OK

- 2** Export the keypair you just generated.

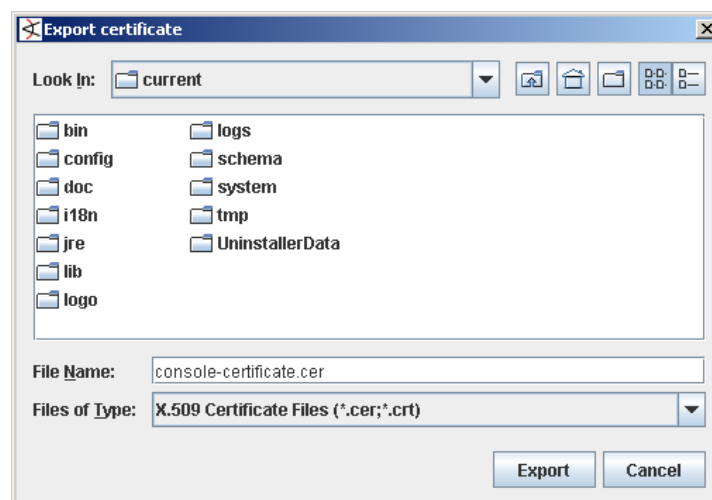
- a In the keytoolgui right-click the keypair you just generated and select **Export** Keypair.



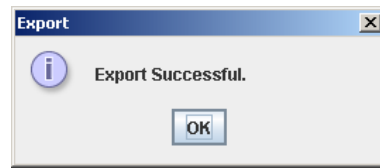
- b Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- 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 key store" on page 38.
- ◆ Use the `changepassword` tool to set an encrypted key store password in the `client.properties` file:

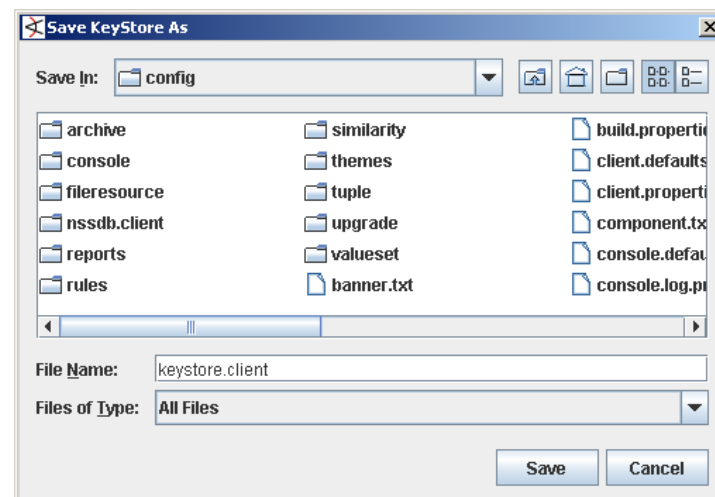
```
arcsight changepassword -f config/client.properties -p
ssl.keystore.password
```

- 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 Give the keystore a name and click **Save**.



- 5 Change the following properties in the Console's `<ARCSIGHT_HOME>/config/client.properties` file and save the file:

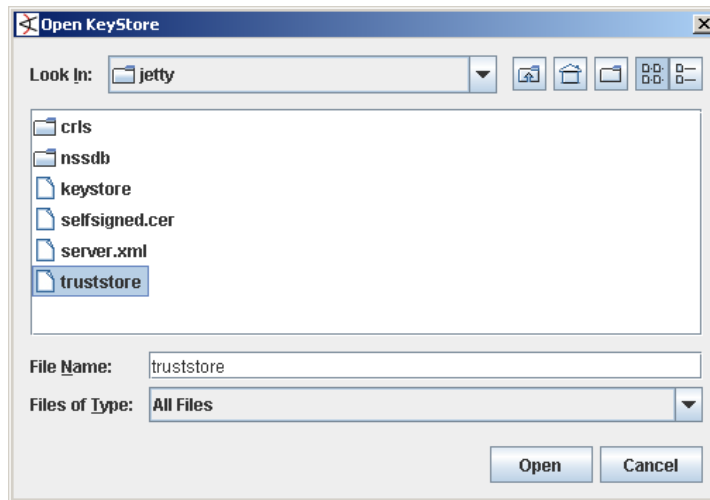
```
ssl.keystore.password=<set-this-to-password-set-when-you-saved-
the-keystore>
```

```
ssl.keystore.path=config/keystore.client
```

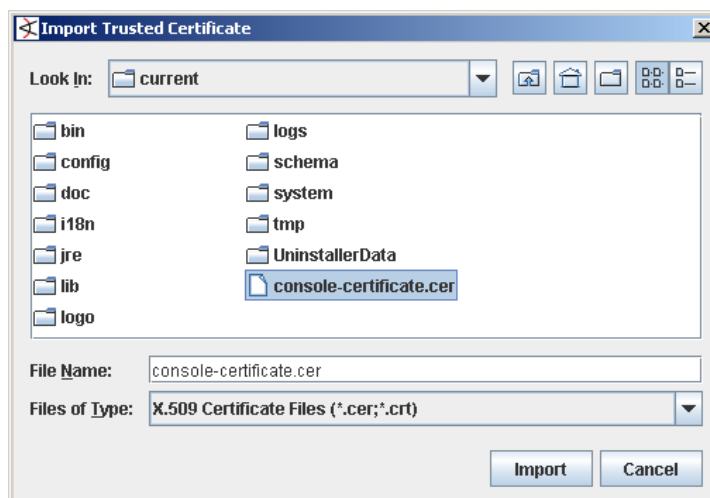
- 6 Import Console's certificate into the Manager's truststore.

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 `<ARCSIGHT_HOME>/config/jetty/truststore`.



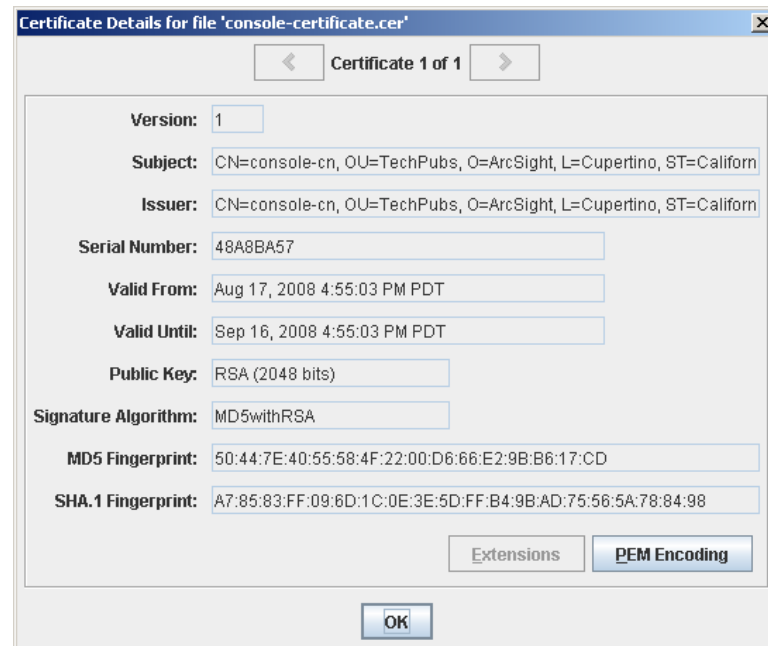
- c Enter "changeit" (without the quotes) when prompted for the password and click **OK**.
- d Click **Tools->Import Trusted Certificate**.
- e Navigate to the Console's certificate that you exported earlier and click **Import**.



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



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



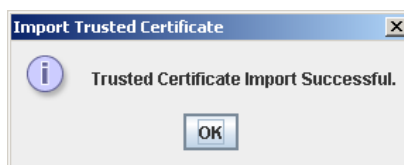
**h** Click **Yes** in the following dialog.



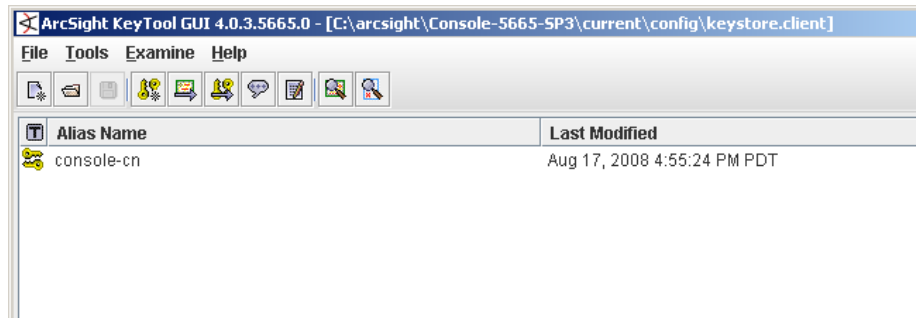
**i** Enter an alias for the certificate.



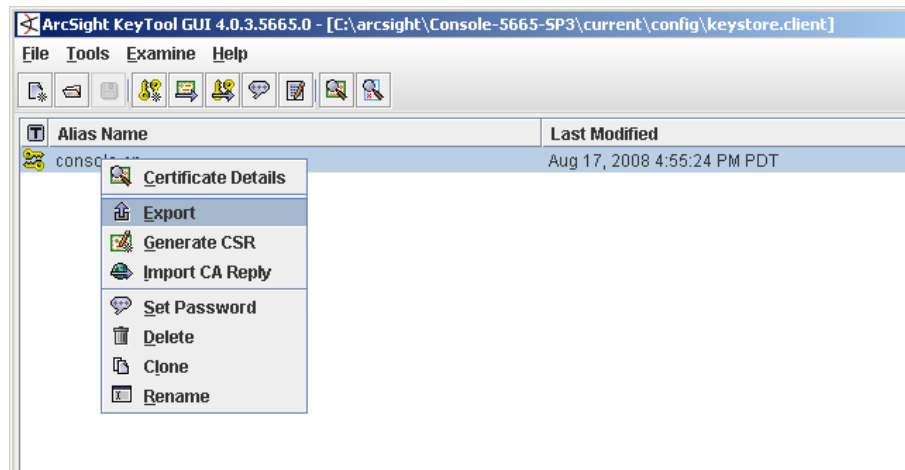
**j** You will get the following message if the import was successful.



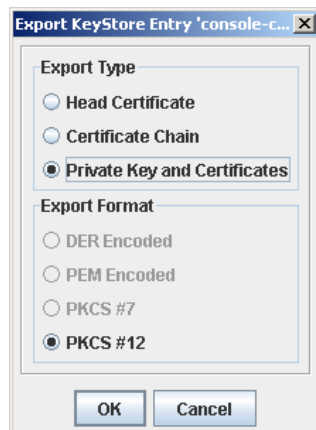
- k Click **OK** and save the changes to the truststore.
- 7 Export the Console's private key. If you use ArcSight Web, you are required to import the Console's private key into the Web browser you use with ArcSight Web.
  - a Start the keytoolgui from the Console's [bin](#) directory.
  - b Click on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



- c Right-click on the Console's keypair and select Export.



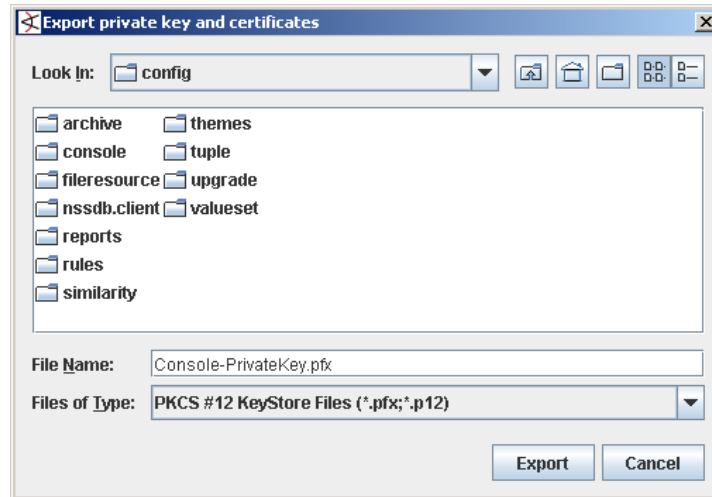
- d Select **Private Key and Certificates** as Export Type and **PKCS#12** as the Export Format if not already selected and click **OK**.



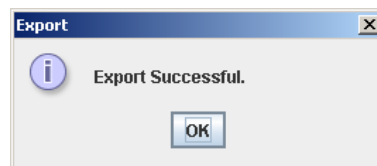
- e Enter the password that you had set for the Console's keystore when prompted and click **OK**.



- 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 running in Default Mode

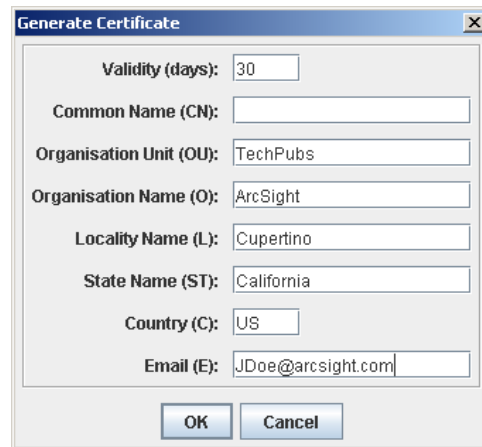
If you want to enable client-side authentication for clients running in default mode, perform these steps in addition to the ones you perform for setting up server authentication:

- 1** Generate a keypair on ArcSight Web. For CA-signed certificate follow the steps in section ["Obtaining a CA-signed certificate" on page 37](#)
  - 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**.

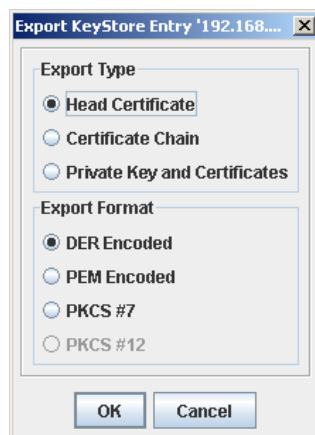


- d Click **Tools->Generate Key Pair** and fill in the fields in the following dialog:

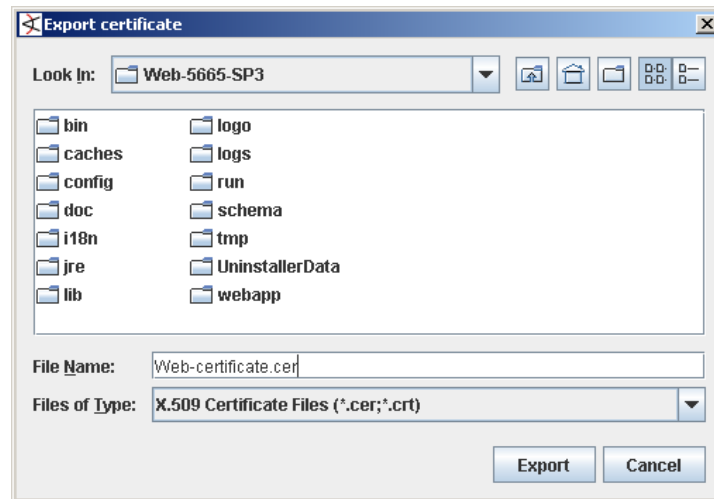


Make sure to use the machine name or IP address on which ArcSight Web is installed for the CN name.

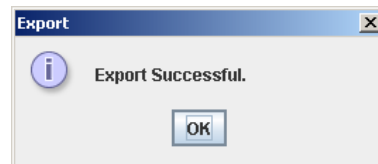
- e Enter an alias for the keypair and click **OK**:
- 2 Export the keypair you just generated.
- a In the keytoolgui right-click the keypair you just generated and select Export Keypair.
- b Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



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



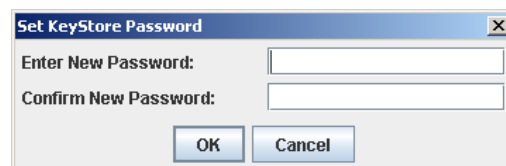
- d You will see the following message:



- 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 key store" on page 38](#).
- ◆ 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:

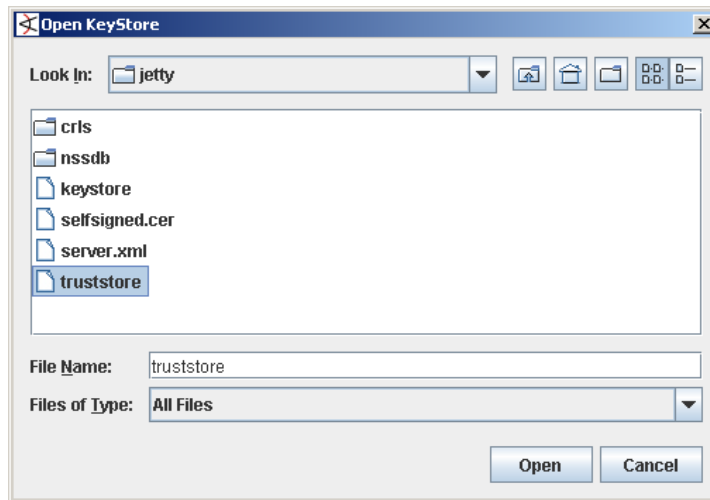
```
ssl.keystore.password=<password-set-when-you-saved-the-
keystore>
```

```
ssl.keystore.path=config/jetty/webkeystore
```

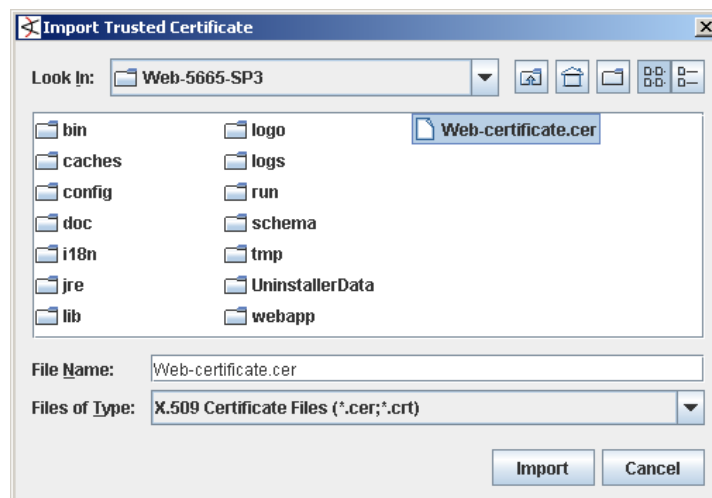
**6** Import Web's keypair into the Manager's truststore.

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**.



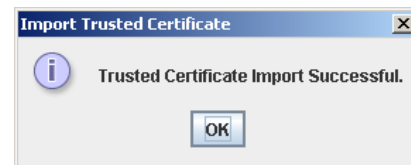
- g** Review the certificate details and click **OK**.

- h** Click Yes in the following dialog.



- i** Enter an alias for the certificate.

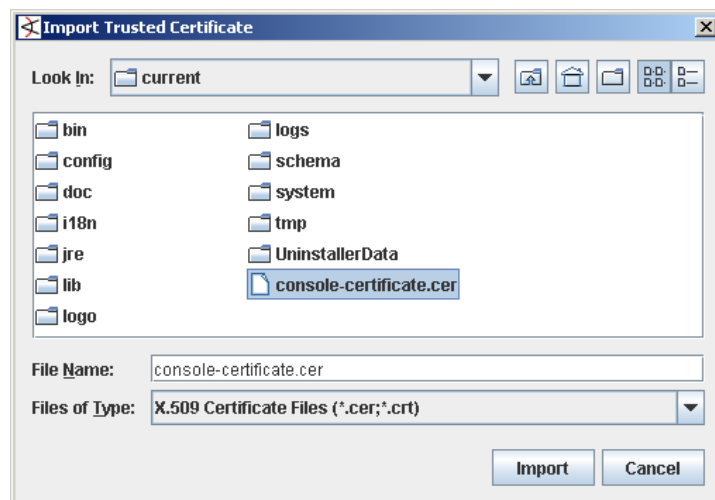
- j** You will get the following message if the import was successful.



- 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 50](#) above.
  - ◆ Console's private key you created in [Step 7 on page 48](#) in section "Setting up SSL Client Authentication on ArcSight Console running in Default Mode" on page 42.
- See your web browser's documentation for steps to do the above.
- 9 Restart the Manager.
- 10 Restart ArcSight Web.

## Setting up SSL Client Authentication for Console running in FIPS Mode



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.

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

- 1 Generate a keypair on the client. Run the following command from the client's `bin` directory:

```
arcsight runcertutil -S -s "CN=<External_ID_of_the_user>" -n
mykey -k rsa -x -t "C,C,C" -m 2345 -d <absolute path to
nssdb.client>
```

where CN is the External ID of the user you created in the Manager's setup and 2345 represents the serial number which has to be unique within the client's `nssdb`.

Make sure you set the alias as `mykey`.

- 2 Export the client's certificate by running the following command from the client's `bin` directory:

```
arcsight runcertutil -L -n mykey -r -d
<full_path_to_nssdb.client> -o
<full_path_to_the_location_where_you_want_to_put_mykey.cert>
```

If you do not specify the full path to the location where you want to export the `mykey.cert` to with the `-o` option, `mykey.cert` will be exported to the client's `<ARCSIGHT_HOME>` directory.

**3** Import the client's certificate into the Manager's `nssdb`. To do so:

- a** Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

This will disable the FIPS 140-2 mode on the Manager's `nssdb` temporarily and allow you to import the Manager's certificate.

- b** Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory to import the certificate into the Manager's `nssdb`:

```
arcsight runcertutil -A -n <aliasname> -t "CT,C,C" -d
<ARCSIGHT_HOME>/config/jetty/nssdb -i
<absolute_path_to_certificate>
```



Make sure that the alias name is any name other than `mykey`. We recommend that you use the external ID as the alias name.

- c** Run the following command to re-enable the FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>/config/jetty/nssdb
```

**4** Run the following from the Manager's `bin` directory:

```
arcsight managersetup
```

**5** When prompted to select a method for authentication, select one of the following:

- ◆ Password Based and SSL Client Based Authentication



ArcSight Web currently does not support this option.

- ◆ Password Based or SSL Client Based Authentication
- ◆ SSL Client Only Authentication

## Setting up SSL Client Authentication for ArcSight Web running in FIPS Mode



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.

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

- 1 Export the Console keypair by running the following command from the Console's `bin` directory:

```
arcsight runpk12util -o
<full_path_to_the_location_where_you_want_to_put_yourconsolecer
t.pfx> -n mykey -d <path_to_nssdb.client>
```

- 2 Import this keypair into the browser. For example, in Internet Explorer:

- a Go to **Tools->Internet Options...**
- b Click the **Content** tab to bring it forward.
- c Click the **Certificates...** button.
- d Select the certificate and click **Import...**

- 3 Import the client certificate into ArcSight Web's webnssdb. To do so:

- a Run the following command from the ArcSight Web's `<ARCSIGHT_HOME>/bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

This will disable the FIPS 140-2 mode on the webnssdb temporarily and allow you to import the client's certificate.

- b Run the following command from the ArcSight Web's `<ARCSIGHT_HOME>/bin` directory to import the certificate into the webnssdb:

```
arcsight runcertutil -A -n <aliasname> -t "CT,C,C" -d
<ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_certificate>
```



Make sure that the alias name is any name other than `mykey`. We recommend that you use the external ID as the alias name.

- c Run the following command to re-enable the FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

## 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 33](#).
- 2 Follow the instructions in ["Verifying SSL Certificate Use" on page 57](#) 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 37](#).



- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 57](#) 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 37](#).
- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 57](#) 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:

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

```
SSL Client
```

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

```
Type JKS
```

```
Demo CA trusted no
```

```
Trusted CA Equifax Secure eBusiness CA-1 []
```

```
Trusted CA VeriSign Class 1 Public Primary
```

```
Trusted CA VeriSign Trust Network [...]
```

```
Trusted CA VeriSign Class 3 Public Primary
.
.
.

Demo CA

Key Store  C:\arcsight\Console\config\keystore.tempca

Exiting...
```

## Changing the Password for keystore/truststore

By default the password for a keystore or truststore is 'changeit' (without the quotes). You can change this password by following the steps below:

- 1 Run the following command from the Manager's `bin` directory:

```
arcsight runmodutil -list -dbdir <full_path_to_nssdb>
```

You can make a note of the token name in the command prompt window.

- 2 Run the following command to change the password for the truststore:

```
arcsight runmodutil -change pw <token_name>
```

Enter your old password and the new password when prompted.

- 3 Update the following in the `server.properties` file located in the Manager's `<ARCSIGHT_HOME>/config` directory.

Change

```
server.privatekey.password.encrypted=<encrypted_password>
```

to

```
server.privatekey.password=<new_unencrypted_password>
```

- 4 Run the `arcsight managersetup` program to encrypt the password.

- 5 If the server certificate exists in the truststore:

- a Remove the certificate from the Manager's truststore by running the following command from the Manager's `bin` directory:

```
arcsight runcertutil -D -n mykey -d <full_path_to_nssdb>
```

- b Create a new Manager certificate by executing the following:

```
arcsight runcertutil -S -s "CN=<hostname>" -n mykey -k rsa -x -t "C,C,C" -m 1234 -d <full_path_to_nssdb>
```

where `hostname` is the name of your Manager machine.

- c Export the newly created certificate from the server:

```
arcsight runcertutil -L -n mykey -r -d <full_path_to_nssdb>
-o <absolute_path_to_mykey.cert>
```



By default, `mykey.cert` will be exported to your `<ARCSIGHT_HOME>/bin` directory if you do not specify the absolute path to `mykey.cert` file destination.

**d** Import the Manager's certificate on all clients:

- i** Temporarily disable the FIPS mode on the client by running the following command from the client's `bin` directory:

```
arcsight runmodutil -fips false -dbdir
<full_path_to_the_client's_nssdb>
```

where `<full_path_to_the_client's_nssdb>` is the path to `webnssdb` on ArcSight Web and `nssdb.client` on ArcSight Console.

- ii** Import the Manager's certificate on the client by running the following command:

```
arcsight runcertutil -A -n mymgrkey -t "CT,C,C" -d
<full_path_to_the_client's_nssdb> -i
<absolute_path_to_mykey.cert>
```

- iii** Enable the FIPS mode on the client by running the following command from the client's `bin` directory:

```
arcsight runmodutil -fips true -dbdir
<full_path_to_the_client's_nssdb>
```

## 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)



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.

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 root certificate is present in the Manager's:
  - ◆ `<ARCSIGHT_HOME>/config/jetty/truststore` directory if the Manager is running in default mode
  - ◆ `<ARCSIGHT_HOME>/config/jetty/nssdb` directory if the Manager is running in FIPS 140-2 mode

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
```

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

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

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 8](#).

### 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= /^\\D.*\\D$/`

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

- `auth.password.regex.match= ^(?!.*[A-Z].*[A-Z])(?!.*[a-z].*[a-z])(?!.*[0-9].*[0-9])(?!.*[^a-zA-Z0-9].*[^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].*[A-Z])(?=[a-z].*[a-z])(?=[0-9].*[0-9])(?=[^a-zA-Z0-9].*[^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 reenabler 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.

## 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 rates 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 253](#).

## 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/System Filters/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.eventName,\
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`.



## 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 72](#)
- [“Monitoring Available Free Space in Tablespaces” on page 73](#)
- [“Setting Up Database Threshold Notification” on page 73](#)
- [“Resetting the Oracle Password” on page 73](#)
- [“Speeding up partition compression” on page 73](#)
- [“Speeding up partition compression” on page 73](#)
- [“Partition logs” on page 74](#)



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.

## 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.compressor.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” on page 249 of the Troubleshooting chapter in this guide.

## Chapter 4

# Managing Resources

---

This chapter discusses the administrator tasks necessary to manage ArcSight ESM.

- [“Managing Users” on page 76](#)
- [“Managing Permissions and Resources” on page 81](#)
- [“Locking and Unlocking Resources” on page 92](#)
- [“Modeling Your Network and Managing Assets” on page 93](#)
- [“Managing Filters” on page 118](#)
- [“Managing Notifications” on page 120](#)
- [“Managing File Resources” on page 126](#)
- [“Managing Packages” on page 129](#)
- [“Managing SmartConnectors” on page 136](#)
- [“Selecting Resources” on page 170](#)
- [“Finding Resources” on page 171](#)
- [“Visualizing Resources” on page 174](#)
- [“Viewing Resources in Grids” on page 177](#)
- [“Validating Resources” on page 177](#)
- [“Extending Audit Event Logging” on page 184](#)
- [“Managing Partitions” on page 184](#)
- [“Managing Customers” on page 188](#)
- [“Saving Copies of Read-Only Resources” on page 189](#)
- [“Using the Image Editor” on page 189](#)
- [“Common Resource Attribute Fields” on page 189](#)

## Managing Users

You manage numbers of users by organizing them into groups based on roles or other logical groupings, setting their permissions and passwords, and enabling or disabling their login functionality. Permissions to access specific ArcSight resources (for example, to create rules or reports) are granted to specific groups by editing the access control lists (ACLs) for those groups.

All ArcSight user group memberships and permissions are stored in the ArcSight Database. When users log in, they are allowed to perform any operations for which they are granted permission through their membership in one or more groups.

## Handling Users

When you create an ArcSight user, that person automatically receives access to a set of resource groups. Users can store, create, edit, or delete resources within their groups without jeopardizing other users' resources.

### Creating a User

- 1 In the Navigator panel drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click the group in which to place the new user and choose **New User**.
- 3 In the **User Editor**, fill in these fields on the **Attributes** tab in the **Login** section:

User Fields	Description
User ID	User name for login ID. This is a required field.
User Type	<p>Choose a user type from the drop-down menu. This is a required field.</p> <p>The currently supported user types are:</p> <ul style="list-style-type: none"> <li>• <b>Normal User:</b> Has full privileges to use the ArcSight Console or ArcSight Web client, and all tools. Only apply this user type to accounts that actually need access to the ArcSight Manager.</li> <li>• <b>Management Tool:</b> Has only the privileges needed to run certain management tools used in conjunction with network management products.</li> <li>• <b>Forwarding Connector:</b> Has only the privileges needed by the ForwardingConnector.</li> <li>• <b>Archive Utility:</b> Has only the privileges needed to run the archive utility. Access to specific resources is controlled through ACLs.</li> <li>• <b>Connector Installer:</b> A specialized identity used only to add SmartConnectors to the system.</li> <li>• <b>Web User:</b> Has privileges to use the ArcSight Web client only (not the ArcSight Console or other tools).</li> </ul> <p>See also <a href="#">"About the System User" on page 79</a>.</p> <p><b>Note:</b> Only users with "Normal User" accounts can log in to the Console or an ArcSight Web client.</p>

User Fields	Description
Login Enabled	<ul style="list-style-type: none"> <li>Select the <b>Login Enabled</b> checkbox to <i>give the user login privileges</i> (a checkmark indicates this feature is <b>on</b>):  <div> <div>Login Enabled</div> <input checked="" type="checkbox"/> </div> </li> <li>Or leave it deselected and <b>off</b> (no checkmark showing) to <i>disable logins</i> for this user:  <div> <div>Login Enabled</div> <input type="checkbox"/> </div> </li> </ul> <p><b>Note:</b> A user account login must be <i>enabled</i> to allow login access to the ESM Console. If you disable a login for a user account, the user cannot log into the Console with the credentials associated with the disabled account.</p>
External User ID	Optionally, provide an alternate, external user ID. (An external user ID might be relevant if you have user accounts from other applications feeding into ESM user database.)
Password	<p>Enter a password for this user. This is a required field.</p> <p>By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.</p> <p>(Passwords can be modified later as a part of editing user information. See <a href="#">"Resetting User Passwords" on page 78.</a>)</p>
Confirm	Re-type the password to confirm it. This is a required field.

**4** Fill in these fields on the **Attributes** tab in the **User** section:

User Fields	Description
Last Name	The user's last name.
First Name	The user's first name.
Title	The user's job title.
Department	The user's department.
Phone	The user's phone number.
Fax	The user's fax number.
E-mail	The user's e-mail address. Use the format user@host.domain. The "@" sign and host domain are required. E-mail addresses are not case-sensitive.
Pager	The user's pager number



For phone, fax, and pager numbers, parentheses (), dashes (-), and periods (.) are allowed. Alphabetic characters are not allowed.

**5** In the **UserID** text field, enter a user login name. This field is required.

**6** Click **OK**.

## Editing a User

- 1 In the **Users** resource tree, right-click the user and choose **Edit User**.
- 2 In the **User Editor**, edit the text fields as described in the table above.
- 3 Grant or withhold login permission by selecting or deselecting the check box next to **Login Enabled**.
- 4 In the **Password** and **Confirm** text fields, edit the user password and confirm it by typing it again. These fields are required.

By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.

- 5 Click **OK**.

## Resetting User Passwords

Administrators may also reset user passwords; for example, if a user's original password has been compromised or you want to make users update their passwords.

- 1 While logged into the Console as an administrator, choose the **Users** resource in the Navigator panel.
- 2 Right-click the user whose password you want to reset and choose **Reset Password**.

The ArcSight Manager assigns a new random password (8 characters, including numbers and letters) and sends it to the selected user's assigned e-mail address.



Be aware that sending a password by email can be dangerous as emails can be intercepted.

---

Alternatively, the following command on ArcSight Manager can be used to reset a user's password:

```
arcsight resetpwd
```

## Moving or Linking a User

- 1 In the **Users** window, navigate to a user and drag and drop it into another group.
- 2 Choose **Move** to move the user or **Link** to create a copy of the user that is linked to the original user.

If you choose **Link**, you create a copy of the user that is linked to the original user. Therefore, if you edit a linked user, whether it is the original or the copy, all links are edited as well. When deleting linked users, you can either delete the selected user or all linked user copies.

## Deleting a User

- 1 In the **Users** resource tree, right-click the user and choose **Delete User**.
- 2 In the dialog box, click **Delete** to delete the user and the listed user's resources or click **Disable Login** to disable the user.



By default, only ESM Administrators have permissions to delete users in a group. If you want to grant non-Administrator users permission to delete users in a particular group, you first need to provide *Write* access to the group by editing access to **User Groups** in the ACL Editor.

Starting with ESM v.4.5 GA, an additional step (providing *Write* access to user Reports) is necessary.

To grant non-Administrator users permissions to delete other users in a group, do the following:

- 1 In the `server.default.properties` file, set the `user.allowmodification=true`.
- 2 Restart the ESM Manager.
- 3 Log into the Console as Administrator, and select the **Users** resource in the Navigator.
- 4 Select the non-administrators group for which you want to provide permissions, right-click, and choose **Edit Access Control** to bring up the ACL Editor.
- 5 On the ACL Editor, click the **Resources** tab.
- 6 Select **Report** in the Resource drop-down menu, and click **Add** to bring up the Reports Selector dialog.
- 7 In the Selector dialog, select all users under `Reports/Shared/Personal/` and click **OK**. All users are shown as Resources targets.
- 8 Click to set **Read (R)** and **Write (W)** permissions as desired (e.g., a checkmark indicates the permission is granted or "on"). Any user in the group now has Edit access to Report groups showing **Write** access (i.e., where **W** is checkmarked), and therefore can delete users in this group.
- 9 Click **Apply** or **OK** to save your changes.

With *Write* permissions enabled on Reports for users you want to delete, members of this group can log into the Console and delete those users.

For more information, see ["Granting or Removing User Group Permissions" on page 85](#).

## About the System User

Starting with ESM v4.0, a special user called the system user is created automatically when ArcSight ESM is installed. This user can lock and unlock ArcSight System Core content.

The system user is configured as 'systemuser' by default. ArcSight recommends that you change this name to a non-standard name. This name can be changed only once. For example, once you change the name to 'coreuser', you cannot change this name again.



ArcSight strongly discourages you from logging in as the system user for regular ArcSight system administration tasks. The purpose of this user is special and its capabilities are limited. For example, the system user cannot use channels or dashboards, install ArcSight SmartConnectors, or log in to ArcSight Web.

## Handling User Groups

User groups associate related users or groups of users. When a group is created within a group, the new group inherits the existing group's permissions.

Groups and users can be managed with drag-and-drop functionality. You can move or copy groups and users into other groups from the Users resource tree. If a group is deleted, the users within that group are also deleted, unless they are also contained by other groups.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

---



You can grant or block non-administrator user access to deploy or un-deploy data monitors. These permissions are configured at the user group level.

For information on how to set user group permissions to enable or disable data monitors, see ["Controlling Who Has Permissions to Deploy Data Monitors" on page 90](#).

---

## Creating User Groups

- 1 On the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click a group and choose **New Group**.  
A name text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

## Renaming User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

## Editing User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

## Moving or Linking User Groups

- 1 In the **Users** resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group or **Link** to create a copy of the group that is linked to the original group.

If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it is the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

## Deleting User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.



## Setting Startup Views

You can define the set of active channel and dashboard resource groups that members of a given ArcSight user group will see by default when they first log in. This includes both Console and ArcSight Web users. These channels and dashboards are initial defaults only: once users begin changing the content of the Viewer panel, the Console and ArcSight Web follow their normal behavior of remembering the most recent state.

The default active channels and dashboards you select for user groups are listed in the User Group Editor on the Startup Views tab.

- 1 Right-click a user group in the Navigator panel's Users resource tree, and choose **Edit Group**.
- 2 In the User Group Editor, click the **Startup Views** tab, then the **Active Channels** or **Dashboards** tabs.
- 3 In either resource tab, click **Add** to open a resource selector dialog box.
- 4 Navigate to and select the appropriate active channels or dashboards to set as users' start-up resources, and click **OK**. Repeat this step to add more resources.
- 5 Click **Refresh** to update the current list of resources, or click **Remove** to take a selected resource off the list. Click **Edit** to change a selected resource in its own editor.
- 6 Click **Apply** to make changes and leave the editor open, or click **OK** to apply your changes and close the editor.

## Managing Permissions and Resources

The subject of managing users is largely that of managing their access to and use of resources.

### Editing Access Control Lists (ACLs)

The user groups ACL Editor has these tabs for viewing or editing permissions on resources, operations, user groups, events, and sortable field sets:

- Resources tab - Lists all resources available to the user group with either inspect or edit permissions, and lets you add/edit resource permissions.
- Operations tab - Lists operations for which this user group has permissions, and lets you add/edit operations permissions. (For example, a user group can have permissions to enable or disable data monitors.)
- User Groups tab - Lists the user groups with either inspect or edit access to the user group itself, and lets you add user groups.
- Events tab - Lists event filters for which this group has permissions, and lets you add/edit event filter permissions. This user group is permitted to see only events from the filters listed on the Events tab.
- Sortable Field Sets tab - Lists sortable field sets for which this user group has permissions. Lets you add/edit field set permissions.



Always remember to have both ArcSight Console and ArcSight Web users log out and back in after changing user or resource access permissions, so they can see those changes.



The Resource ACL display shows relationships between users and groups, and how permissions are acquired for each of the user groups. Child groups inherit permissions from parent groups.

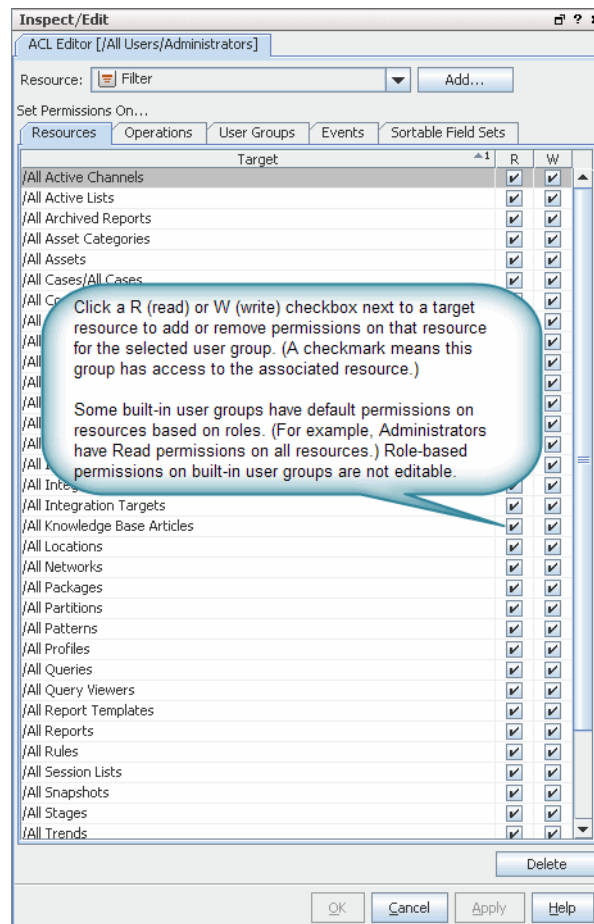
For example, consider the following scenario.

- A user logged in as Administrator (belonging to the group /All Users/Administrators) has read and write permissions by virtue of being in the Administrators group.
- All users have read permissions because they belong to the group /All Users/Default User Groups by default.
- A user logged in as an Analyzer Administrator has both read and write permissions because they inherit read permissions from the parent group (/All Users/Default User Groups) and get write permissions per the Analyzer Administrators child group.

## Granting or Removing Resource Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Resources** tab.

The Resources tab lists all resources available to this user group with either inspect (**Read**) or edit (**Write**) permissions, and lets you add/edit resource permissions. Available resources are listed based on *user permissions*, so some might not show.



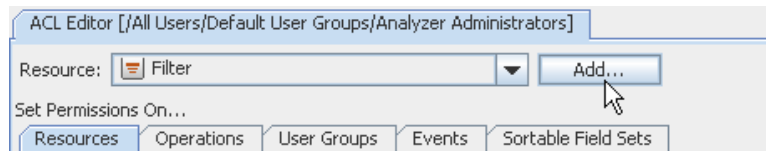
- 5 Add or remove permissions on a resource for this user group as follows.

- ◆ **To edit permissions on a resource *shown in the current list***, click the **(R)** read or **(W)** write checkbox next to a target resource to add or remove permissions on that resource.

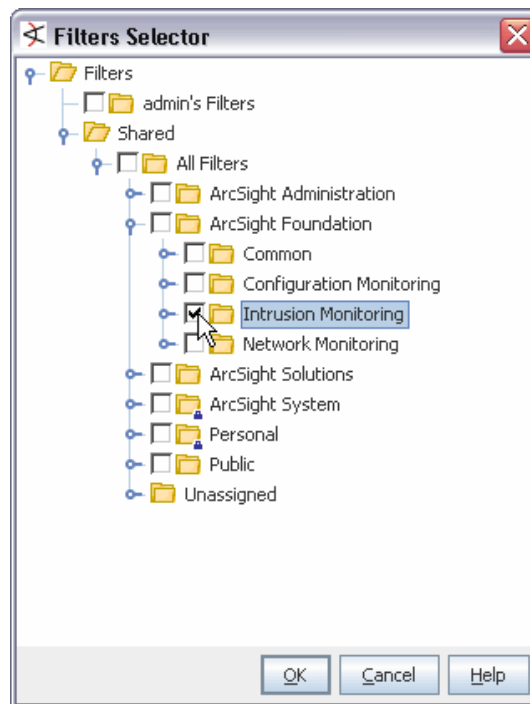
A checkmark means that this user group has access to the associated resource. A blank checkbox means this group does not have access to the resource.

Target	R	W
/All Active Channels	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/All Active Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ◆ **To add permissions for a resource *not shown in the current list***, select a resource from the Resource drop-down menu at the top of the Resources tab and click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the resources you want to add permissions for and click **OK**.



The resource you added will be listed as a target on the Resources tab and then you can edit its **Read/Write** permissions as needed.

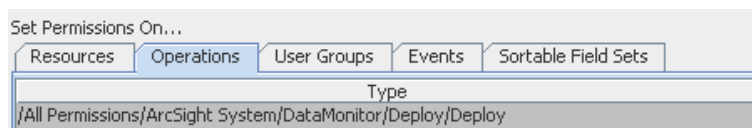
- ◆ To remove a resource from the list (and **remove all permissions on it** for this group), select the resource in the list and click **Delete**. (The Delete button is at the bottom of the Resources tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Resources permissions.

## Granting or Removing Operations Permissions

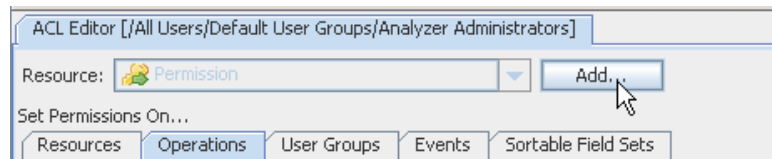
Starting with ESM 4.5, data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions by setting permissions on this particular “operation”. For ESM v.4.5, the only operation available to set permissions on is data monitor deployment. It is likely that fine-grained permissions control will be added for other operations as needed. (See also, [“Controlling Who Has Permissions to Deploy Data Monitors” on page 90.](#))

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Operations** tab.

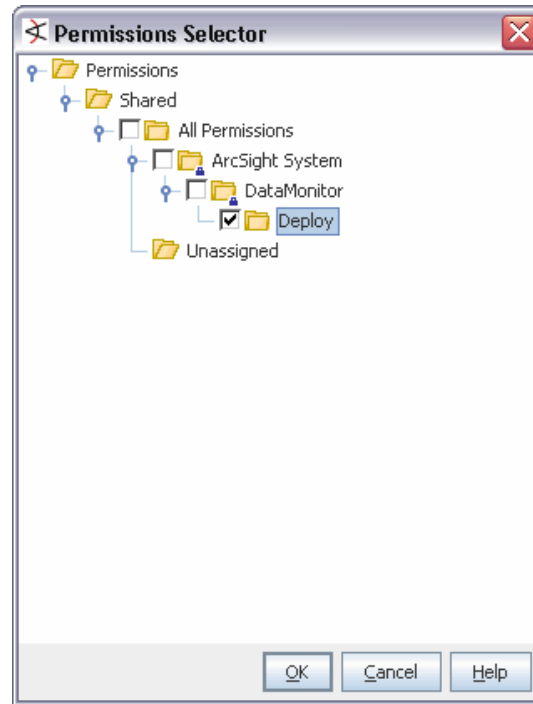
The operations for which this user group has permissions (if any) are listed.



- 5 Add or remove user group permissions to perform an operation as follows.
  - ◆ To add permissions to perform an operation not listed, click **Add**.



Select the operations you want to add permissions for and click **OK**.



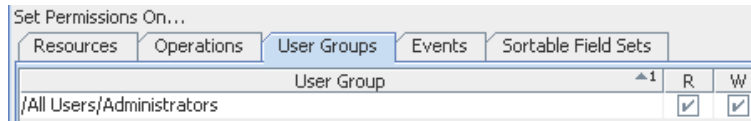
The list of Operations is updated to include the one you added. Operations listed are those this user group has permissions to perform.

- ◆ **To remove permissions to perform an operation**, select the operation in the list and click **Delete**. (The Delete button is at the bottom of the Operations tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

## Granting or Removing User Group Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **User Groups** tab.

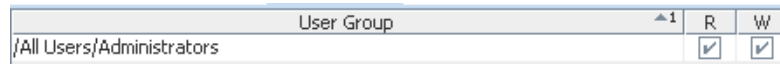
The User Groups tab lists all user groups for which members of the selected group have inspect (**Read**) or edit (**Write**) permissions, and lets you add/edit group permissions.



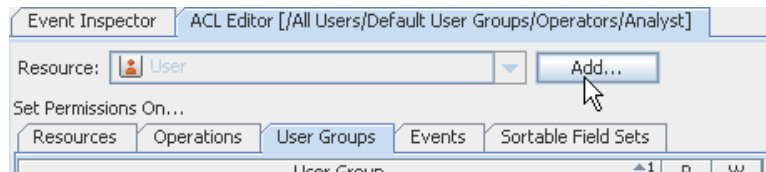
This is where you grant or deny members of the group you are editing permissions to edit their own user groups. Depending on your own user permissions, some user groups may or may not be shown, and Read/Write checkbox options may or may not be editable.

- 5 Add or remove permissions on a user group as follows.
  - ◆ **To edit permissions on a user group *shown in the current list***, click the **(R)** read or **(W)** write checkbox next to a target resource to add or remove edit permissions on that user group.

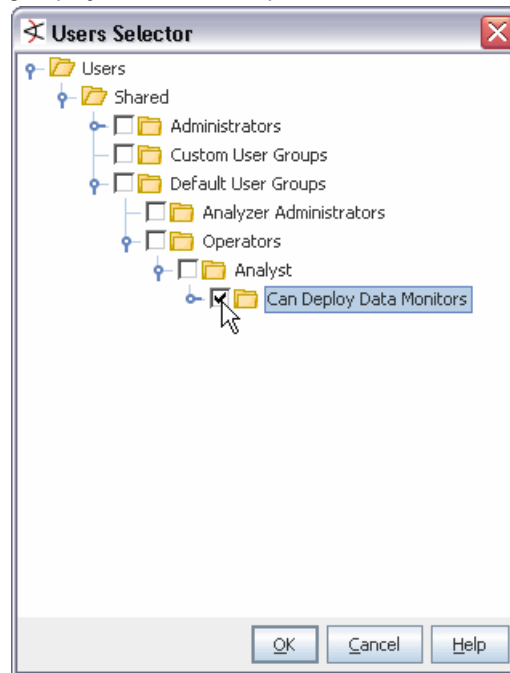
A checkmark means that this user group can edit permissions on the associated group. A blank checkbox means this group does not have edit permissions on it.



- ◆ **To add permissions on a user group *not shown in the current list***, click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the groups you want to add permissions for and click **OK**.



The user group you added is now listed on the User Groups tab and then you can edit its **Read/Write** permissions as needed.

User Group	R	W
/All Users/Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Users/Default User Groups/Operators/Analyst/Can Deploy Data Monitors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

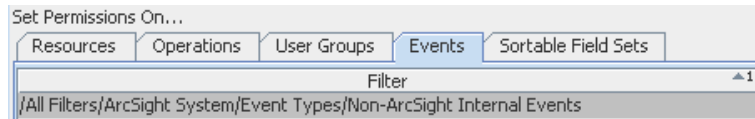
- ◆ To remove a user group from the list (and **remove all edit permissions on it**), select the user group in the list and click **Delete**. (The Delete button is at the bottom of the User Groups tab).

- 6 Click **OK** on the User Group ACL Editor to save changes to User Group permissions.

## Granting or Removing Event Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Events** tab.

The *event filters* that return the types of events for which this user group has permissions are listed.



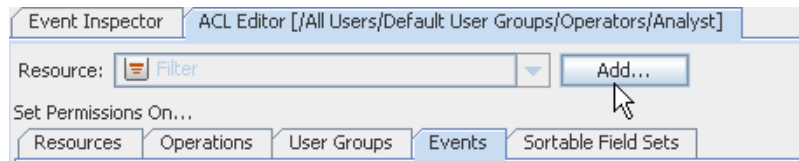
User groups are granted permissions to events by means of event *filters* applied to groups. The event filters limit the types of events group members can access through the ESM Console.

For example, members of the ESM Administrators group can view all events, as indicated by the event filter assigned to the Administrators group by default: `/All Filters/ArcSight System/Core/All Events`.

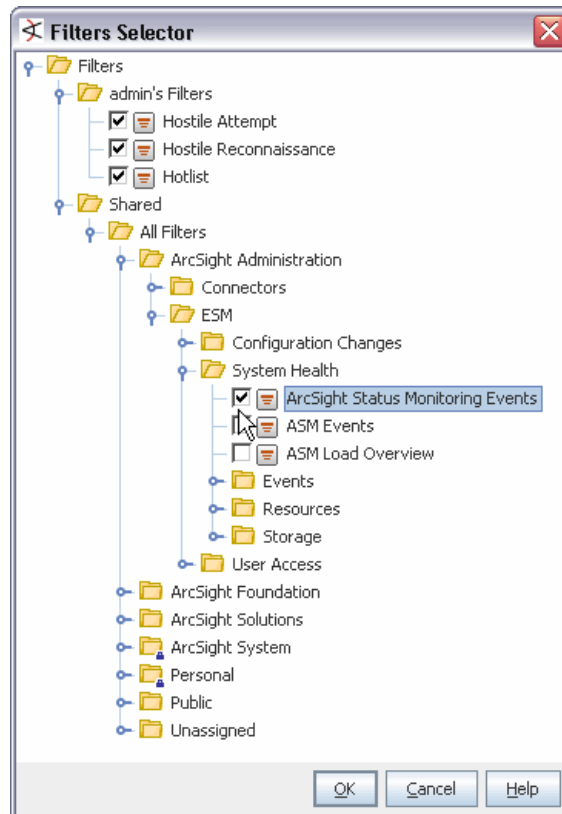
For more information about events, see “Monitoring Events” in the ESM User’s Guide or the Console Help.

## 5 Add or remove user group permissions to view events as follows.

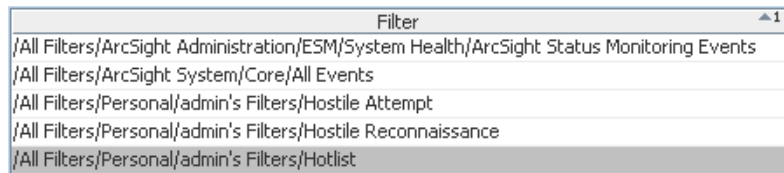
- ◆ **To add permissions to view events** captured by a filter not shown in the current list, click **Add**.



Select the event filters you want to add permissions for and click **OK**.



The list of event filters is updated to include the ones you added. Filters listed capture and allow all event types this user group has permissions to view.



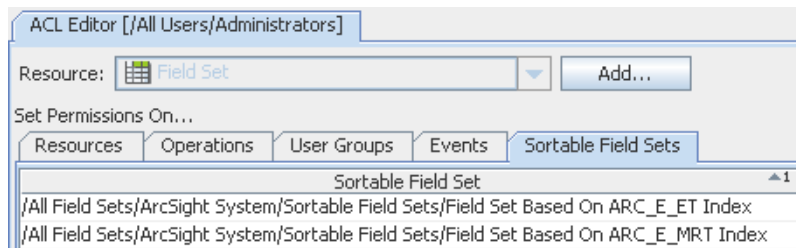
- ◆ **To remove event filters** (permissions to view certain types of events), select a filter in the Events “Filter” list and click **Delete**. (The Delete button is at the bottom of the Events tab).

- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

## Granting or Removing Sortable Field Sets Permissions

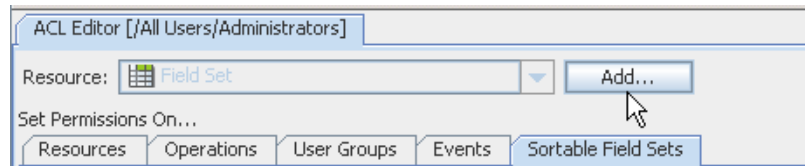
- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Sortable Field Sets** tab.

The event field sets for which this user group has access permissions are listed.



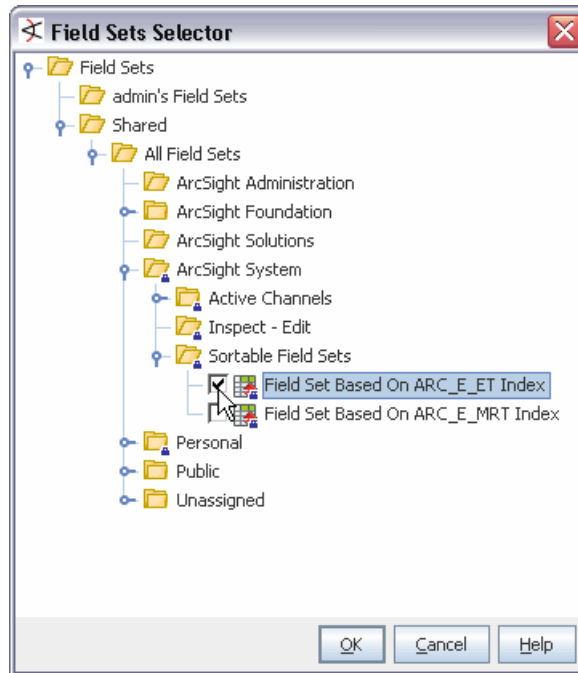
- 5 Add or remove user group permissions on sortable field sets as follows.

- ◆ **To add permissions to use a field set** not shown in the current list, click **Add**.





Select the sortable field sets you want to add permissions for and click **OK**.



The list of sortable field sets is updated to include the ones you added. Field sets listed represent those this user group has permissions to use.

- ◆ **To remove sortable field sets**, select a field set in the list and click **Delete**. (The Delete button is at the bottom of the Sortable Field Sets tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Sortable Field Sets permissions.

## Sharing Resources

You can share your resources with other users by moving, copying, or linking your resource to or into another resource's Public group; for example, to share a filter you would move it into the Public Filters group in the Filters resource tree.

### To share a resource

- 1 In a resource tree, drag a resource and drop it into the Public group (this can be a single resource or a resource group).
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the resource that will not be affected when the original resource is edited. If you choose **Link**, you create a copy of the resource that is linked to the original resource. Therefore, if you edit a linked resource, whether the original or the copy, all links are edited as well. When deleting linked resources, you can either delete the selected resource or all linked resources.

You can also multiple-select resources with the **Shift** key, and drag-and-drop or keyboard copy-and-paste, to move, copy, or link them in another group.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

## Controlling Who Has Permissions to Deploy Data Monitors

Starting with ESM 4.5, data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions.

Depending on the permissions associated with the user group to which they belong, users may or may not have options available on their consoles to **Enable** (*deploy*) or disable (*un-deploy*) data monitors.

Administrators (all users belonging to the [admin](#) user group) have permissions to deploy/undeploy data monitors.

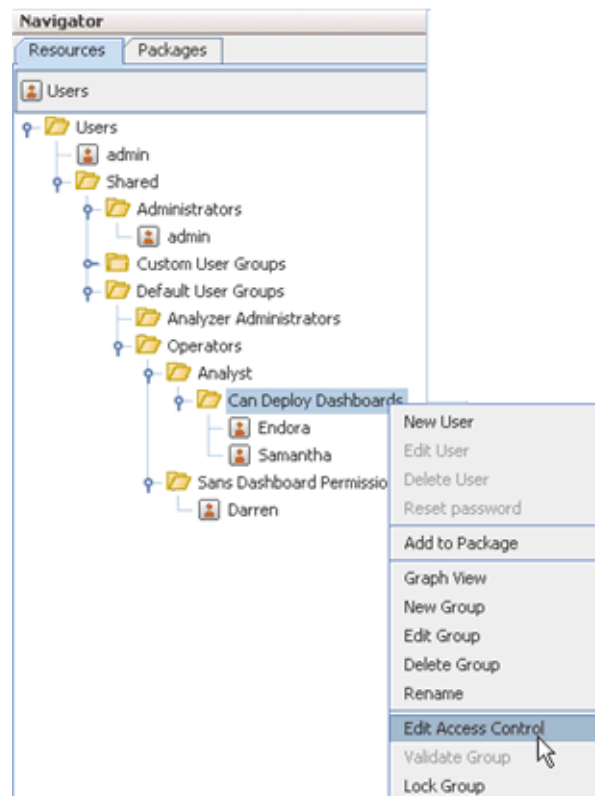
Administrators can grant permissions to deploy/undeploy data monitors to other non-Administrator through the Users resource Access Control Lists (ACLs) editor, as described in [“Granting or Removing Operations Permissions” on page 84](#). As with user permissions for other resources, these are applied at a user group level. As an administrator, you can grant all users in a given group permission to deploy data monitors. Once user groups are set up and appropriate permissions applied to those groups, you can add new users to appropriate groups, and change access permissions for existing users by moving them in or out of various groups. If you want to allow or disallow a particular user the option to deploy data monitors, move the user in or out of a group that has that permission.

To configure data monitor deployment permissions:

- 1 If needed, set up one or more user groups for non-admin users to whom you want to control permissions to deploy data monitors. (For example, at the simplest level you might have a group for analysts and operators who are allowed to deploy data monitors and another for those you want to block from this option.)

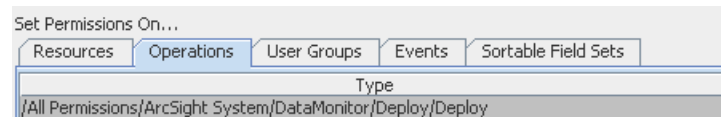
See [“Handling Users” on page 76](#) and [“Handling User Groups” on page 79](#) for information on adding, deleting, and editing users and user groups.

- 2 Follow the instructions provided in [“Granting or Removing Operations Permissions” on page 84](#) to grant or remove permission to deploy data monitors to a particular group. As a part of these instructions, you'll select the **Users** resource in the navigator, right-click a group and choose **Edit Access Control**.



- 3 In the ACL Editor, click the Operations tab, and click **Add**.
- 4 On the Permissions Selector, select **Deploy** under **Permissions\Shared\All Permissions\ArcSight System\Data Monitor\** and click **OK** to save the settings and close the dialog.

The list of Operations is updated to include deployment permissions on data monitors.



(To remove the permission for this group, select the permission and click **Delete**.)

- 5 Click **OK** on the ACL Editor to save your changes.

For more information on administrator tasks of working with user permissions and ACLs, see [“Managing Permissions and Resources” on page 81](#).

## How Upgrades Affect Data Monitor Deploy Permissions

Upon installation and deployment of a different version of ESM software (e.g., version or service pack upgrades), only administrators (**admin** users) will keep permissions to deploy/undeploy data monitors. Non-**admin** users will not have deploy permissions on data monitors even if they had such permissions as part of the previous ESM configuration.

After upgrades, all users will have access to already-deployed data monitors. But, initially, non-[admin](#) users will not have permissions to enable/disable data monitors, nor have access to new data monitors unless an administrator enables (deploys) these.

To re-establish data monitor deployment permissions for non-[admin](#) users after an upgrade, administrators can reconfigure fine-grained permissions. They can re-group users and perhaps link non-[admin](#) users into existing or new groups with more permissions (like data monitor deployment), as described in [“Controlling Who Has Permissions to Deploy Data Monitors” on page 90](#).

## Deployment Permissions on Imported Data Monitors

If a user without data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import will succeed but the data monitor will be disabled (*undeployed*). After the import, the user will not have permissions to deploy the data monitor unless an administrator reconfigures permissions for that user.

If a user with data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import will succeed and the data monitor will keep its enabled (*deployed*) setting. After the import, this user will be able to view the data monitor and re-set its deployment state as needed.

## Locking and Unlocking Resources

The locking and unlocking capability applies to the following ArcSight content:

- System core content
- User created content

### System Core Content

When you install the ArcSight ESM system, a set of predefined content called the System Core content is installed by default. This content provides the foundation building blocks for the ArcSight ESM to work.

System Core content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in [/All Filters/ArcSight System/Core](#).

The modification of System Core content can adversely impact the operation of ESM, therefore, it is locked by default. ArcSight strongly recommends against unlocking or modifying this content. If there is a need to unlock this content, contact ArcSight Customer Support.



Use the resources available in ArcSight Foundation packages or ArcSight Administration to create content to suit your needs.

---

### User Created Content

ArcSight users can lock any resource or a group of resources to which they have write access privileges. Locking prevents a resource from being modified or deleted. Once locked, such resources or groups can be unlocked only by these users:

- The user who applied the lock—the lock owner.

- Any user who has write permissions to the lock owner. That is, a user who has privileges over the user who applied the lock. For example, the administrator user has write permissions over all users by default. Therefore, if user joe locks a resource, the user administrator can unlock it.
- The system user.



You can make a copy of a locked resource even if you do not have the privileges to unlock it.

You can edit resources in a locked group if you have write access privileges to the resource, however you cannot do the following:

- Delete or remove resources from it.
- Add a new resource to it.

## Unlocking a User-locked Resource

To unlock a resource, right click the locked resource and select **Unlock** from the drop-down menu. For detailed instructions, see the Console online Help.

## Modeling Your Network and Managing Assets

ArcSight ESM operates on a data model that enables you to build a business-oriented view of data derived from physical information systems. These distinctions help ESM clearly identify the events in your network, and provide more layers of detail to ESM correlation capabilities. Modeling your network and the assets it includes is part of ESM setup and ongoing maintenance.

The following topics provide a conceptual overview of network asset modeling, and describe how to configure, update, and maintain a network model in ESM.



- For a description of techniques for dealing with hundreds of thousands of assets, see [“Asset Scalability” on page 113](#) in this guide.
- For a more detailed conceptual overview, information about configuring each type of ESM asset and modeling your network, refer to the *ArcSight ESM 101* chapter on the “ESM Network Model.”

## Network Model

The network model is a representation of the nodes (*assets*) on your network and certain characteristics of the network itself.

Before you can make an informed decision about what to do about a particular event, it helps to know something about the event's source and destination. Is the source a previous attacker, does it come from a hostile region of the world, or is it a trusted server that has suddenly become the source of a hostile attack? Does the destination expose relevant vulnerabilities, does it host critical applications, or is it a known server of forbidden services?

ESM captures this kind of information by modeling the assets on your network and particular attributes of the network itself that are pertinent to ESM. The network model represents information for individual assets and whole zones.

For critical assets on the protected network, network modeling captures important facts that will help inform your decisions, such as:

- All open ports
- The operating system running on that host
- Known vulnerabilities that might be exposed
- Applications present
- The missions these applications support and their criticality to your operation

For less critical assets, such as a particular block of addresses on the Internet, it may be sufficient to just know general information about them, such as the country in which those assets reside.

## Populating the Network Model with Assets

There are several ways you can populate the network model with assets. Most enterprises use a combination of these methods:

- **Manually, using ESM network modeling tools (assets resources):** Set every parameter for every asset manually using ESM's network modeling tools.
- **Use the ESM Network Model wizard:** Starting with ESM v.4.5, a Network Model wizard is provided on the ESM Console (menu option **Tools > Network Model**). For more information, see ["Populating the Network Model Using the Wizard" on page 97](#).
- **Automatically, from a vulnerability scanner:** Use the output of a vulnerability scan, such as FoundStone, ISS Internet Scanner, or Nessus, as reported to the ESM Manager from a scanner SmartConnector. You can configure an SmartConnector to import the data from the vulnerability assessment tool. ESM converts the data into the ESM format.

You can use a vulnerability scanner to populate the baseline network model, or you can import network model data as a `.csv` file. Scanners cannot populate zones or asset ranges, however, so once scanner data is imported, you can use the ESM network modeling tools to manually fill in the model with these distinctions.

For details about how to import an existing network model as a `.csv` file, see ["Uploading Files and Creating a File Resource" on page 126](#).

- **Import network model from an existing configuration database:** Many enterprise networks have third-party systems that already model the properties of the assets on your network. You can export these network models, translate the format into the ESM schema using a utility supplied by ArcSight, and import it to the ESM Manager as a resource archive with the help of ArcSight Professional Services.

ESM uses the following objects to model the network. These are represented as *resources* on the ESM Console, as described in ["Understanding ESM Asset Resources" on page 95](#).

- **Assets** represent individual nodes on the network, such as servers, routers, and laptops.
- **Asset ranges** represent a set of network nodes addressable as a contiguous block of IP addresses.
- **Zones** represent portions of the network itself and are also characterized by a contiguous block of addresses.
- **Networks** provide an additional distinction to differentiate between two private address spaces with overlapping IP address ranges.
- **Customers** describe the internal or external cost centers or separate business units associated with networks, if applicable to your business environment. Customer tagging is a feature developed mainly to support Managed Service Security Provider (MSSP) environments, although it can also be used by private organizations to denote cost centers, internal groups, or subdivisions. The Customer designation keeps event

traffic from multiple cost centers and/or business units clearly identified and separate. A customer can be thought of as the "owner" of an event, rather than the source or target of an event.

## Understanding ESM Asset Resources

The **Assets** resource in the Navigator panel contains subtabs for the following network modeling resources:

### Assets

An asset is any network endpoint with an IP address, MAC address, host name, or external ID. For network modeling purposes, an asset is any endpoint you consider significant enough to characterize with details that will make ESM correlation and reporting more meaningful.

ESM automatically creates assets to model the network nodes that host ArcSight components (Managers, Databases, Consoles, and SmartConnectors). It also automatically creates assets for events received from device endpoints on your network that do not already have assets modeled in ArcSight. This auto-asset creation feature could require configuration, depending on the assets reporting in to ESM. For more about this feature and how to configure it see:

"Configure Asset Auto-Creation Filters" in "ArcSight Express Solution" in the ESM User's Guide or Console HelpAssets can be populated using any of the following methods:

- Manually using the Console
- Using the Network Model wizard
- Dynamically from scanner data

### Locations

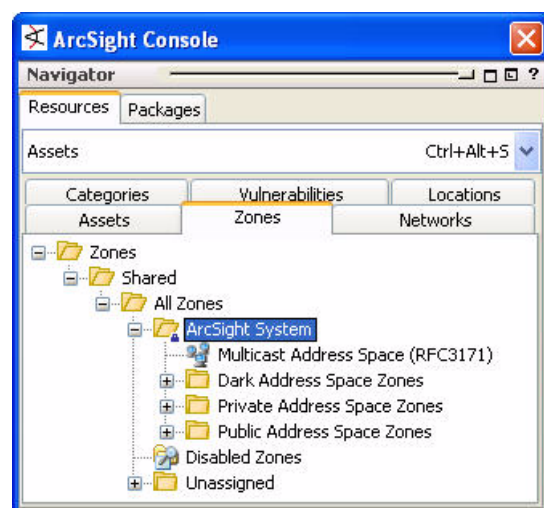
The locations designated to help sort out and identify the physical deployment of various assets are usually set during ArcSight deployment. Ordinarily, you do not need to change these assignments unless you need to reflect a reorganization or a renaming project. While you create locations through the Location Editor, you assign them to assets through the Asset Editor. Each asset can be assigned to only one location. You can also assign locations to zones and networks. Private address-space zones, in particular, should be associated with locations.

### Zones

Zones are ArcSight resources that represent a functional part of the network with contiguous IP addresses, such as DMZ, VPN, wireless LAN, or DHCP.

With ArcSight v4.0, every asset or address range is associated with a zone. ArcSight comes configured with the standard global IP address ranges already represented as zones, so if your network uses only these public IP addresses, ArcSight can resolve them without setting up any additional zones.

ESM comes with the following standard zones:



You would need to create your own zones if you have overlapping private networks. Private networks usually model a functional group within your network or a subnet, such as a wireless LAN, the engineering network, the VPN or the DMZ.

For details about using the zone editor, see [“Zone Editor” on page 109](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 108](#).

## Networks

Networks are ArcSight resources that are used to differentiate between zones whose IP ranges overlap, such as when branch locations assign the same private address spaces to resources in their locations.

ESM comes configured with two standard networks: Local and Global.

The standard “Global” network automatically recognizes the available zones and provides the correct addressing information to ArcSight SmartConnectors when they are installed. Custom Networks are also used to compartmentalize customer entities in MSSP situations. When you associate a customer or a location with a network in the Network Editor, zones automatically access this information. (See [“Network Editor” on page 110](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 108](#).)

## Vulnerabilities

The asset vulnerabilities on your network are normally discovered and updated automatically by scanners. The most common manual change to a vulnerability resource is to associate it with a Knowledge Base article. You can associate assets with vulnerabilities from either the Vulnerabilities or Assets editors. (See [“Vulnerability Editor” on page 110](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 108](#).)

## Asset Categories

Asset categories are ArcSight resources that describe the properties of an asset in terms of how it is used. Asset categories are one of the key ways that ESM adds differentiation, relevance, and context to the millions of events passing through your network.

Asset categories establish identity, ownership, and criticality of the assets on your network. Asset categories present an extensible schema that adds value to the business properties of your assets. The root of a particular category (for example, **Criticality** in the group



[/All Asset Categories/System Asset Categories/Criticality](#)) defines the property itself, whereas the members of the category (for example, the criticality levels [Very High](#), [High](#), and so on) define the possible values for that property.

You can create new categories through the Group Editor, and associate categories with assets through the Asset Editor. One asset can fall into multiple categories. You can also apply categories to zones. (See [“Categories” on page 110](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 108](#).)



Always exercise caution when deleting or changing existing asset categories. For safety, create new categories in new folders.

For more information about asset categorization and categories in ESM, see the ESM User's Guide and/or Console Help.

## Populating the Network Model Using the Wizard

Starting with ESM v.4.5, a Network Model wizard is provided on the ESM Console (menu option **Tools > Network Model**). The Network Model wizard provides the ability to quickly populate the ESM network model by batch loading asset and zone information from Comma Separated Files (CSV) files. The following data can be imported into an ArcSight ESM Manager from CSV files:

- **Zones** define functional parts of a network, such as a wireless LAN, an engineering network, a VPN or a DMZ. For the column types of the zones CSV file, see [“Zones CSV File Format” on page 100](#).
- **Assets** represent individual nodes on the network, such as servers and routers. For the column types of the assets CSV file, see [“Assets CSV File Format” on page 101](#).
- **Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. Asset ranges should be a subset of the IP address ranges defined for zones. For the column types of the asset ranges CSV file, see [“Asset Ranges CSV File Format” on page 103](#).

You can import combinations of input CSV files at one time using the Network Model wizard but only one file of each type can be imported during a single import. For example, if you only have assets to import, you can import only an assets CSV file. If you have a zones CSV file, an assets CSV file, and an asset ranges CSV file to import, you can import all three at once using the Network Model wizard.

## Specifying CSV Column Types

Each CSV file type defines a set of required column(s) and optional columns. In addition, the CSV file can contain columns that are not used by the Network Model wizard. The columns can be in any order but the Network Model wizard requires that you specify the types of each column so the wizard knows how to interpret each column. You can specify the column type using one of the following methods:

- Specify the column type in the header of the CSV file itself, prior to launching the Network Model wizard. For instructions, see [“Specify the Column Type Using a Header” on page 98](#).
- While running the Network Model wizard, assign the appropriate column type for each column in the Select Column Headers panel. For instructions, see [“Assign the Column Type in the Wizard” on page 99](#).

Columns not used by the Network Model wizard must be assigned the column type **Ignore**. Only columns of type **Ignore** and **Category URI** can be repeated in the CSV file. For all other column types, only one instance of the column type can be assigned in the file. For example in a zones CSV file, only one column should be assigned the **Name** column type. If duplicate columns of a non-repeatable column type exist in the CSV file, one of the columns should be assigned the **Ignore** column type. For example if two name columns appear in the CSV file, one should be assigned the **Name** column type and the other should be assigned the **Ignore** column type.

### Specify the Column Type Using a Header

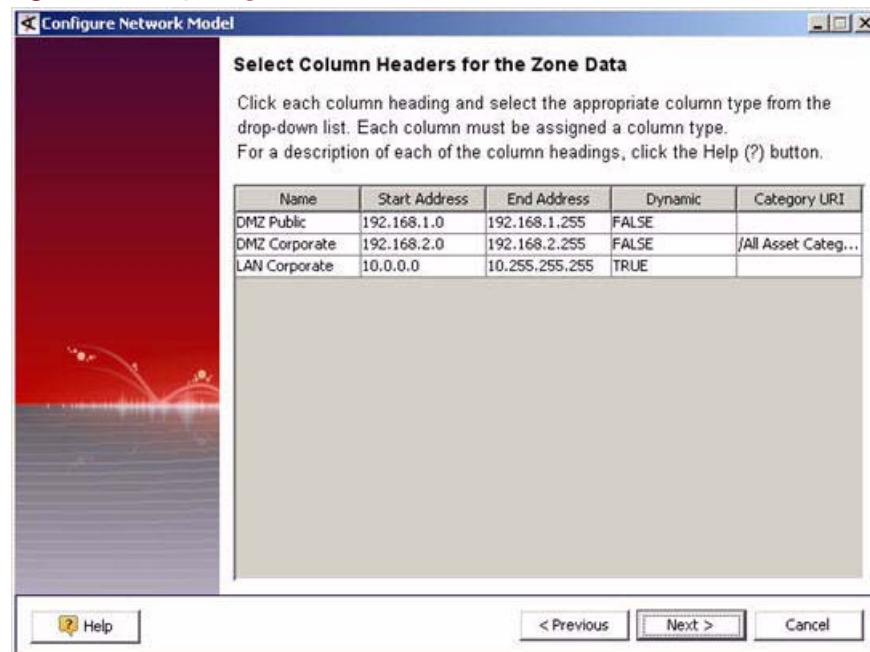
In this method, you specify the column type in the first row (header) of the CSV file itself before importing the CSV file using the wizard. The column name in the header must match the column type specified in the [Table 4-1, "Zones CSV File Format," on page 101](#), [Table 4-2, "Assets CSV File Format," on page 102](#), or [Table 4-3, "Asset Ranges CSV File Format," on page 104](#).

As shown in following sample zones CSV file, the column names in the first row (highlighted in **bold**) match the column types specified in [Table 4-1, "Zones CSV File Format," on page 101](#). The wizard determines how to interpret each column using the column type specified in the header.

```
Name,Start Address,End Address,Dynamic,Category URI
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```

When this zones CSV file is imported into the wizard, the wizard correctly matches the column types because the column types have been correctly specified in the header, as shown in [Figure 4-1](#).

**Figure 4-1** Importing Zones CSV File with Header Row

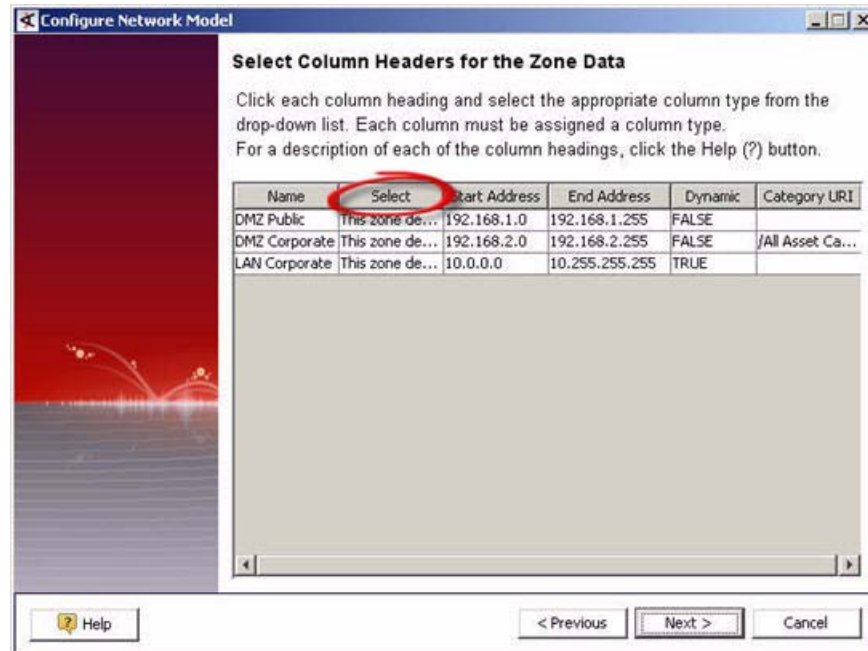


### Assign the Column Type in the Wizard

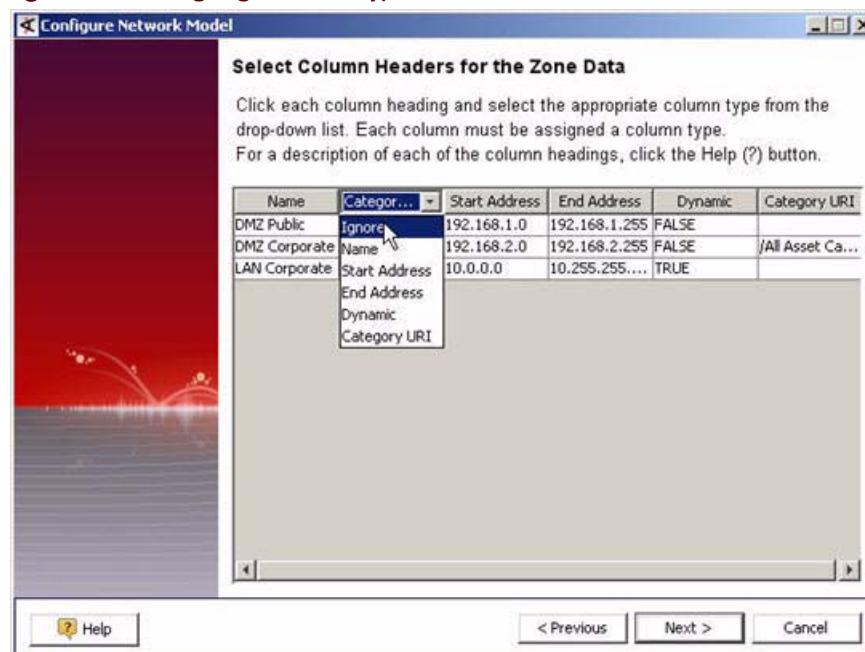
In this method, you assign the column type in the Select Column Headers panels while running the wizard. When the following sample zones CSV file (which does not contain a header row) is imported, the wizard does not know how to interpret all the columns as shown in Figure 4-2.

```
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```

**Figure 4-2** Importing Zones CSV File without Header Row



By default, when this sample data is imported into the wizard, the second column is automatically assigned to the [Select](#) column type but the second column is a description of the zone and should be assigned the [Ignore](#) column type. To change the column type, click the title of the column and from the drop-down menu select the appropriate column type as shown in Figure 4-3.

**Figure 4-3** Assigning a Column Type

## Zones CSV File Format

Zones define functional parts of a network, such as a wireless LAN, private networks, or subnets. For example, the following network areas could be identified as a zone: the VPN, the DMZ, or an engineering network. Zones are identified with a contiguous block of addresses.



Each zone should specify a unique range of IP addresses. The IP addresses specified by zones should not overlap. If you import a zone that overlaps with a zone already specified on the ArcSight ESM Manager and the new zone has a different name than the existing zone, the following occurs:

- the new zone is created
- the existing zone is invalid and displays with the broken zone icon in the ArcSight ESM Console

You can define a set of zones in ArcSight ESM by batch loading zone definitions from an zones CSV file. Zone CSV files contain the columns listed in [Table 4-1 on page 101](#). When a zones CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Zone Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 104](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 97](#).

When the Next button is clicked in the Summary of Data to Import panel, the zone data is imported into the ArcSight ESM Manager. The new zones are created in the [/All Zones/Site Zones](#) group. For example, if a zone called [DMZPublic](#) was specified in the imported zones CSV file, a new zone is created at the following URI: [/All Zones/Site Zones/DMZ Public](#). The new zones are assigned to the default network called [Local](#).

**Table 4-1** Zones CSV File Format

Column Type	Description	Required Column?	Repeatable Column?	Example Value
<b>Name</b>	A descriptive name for the zone such as the purpose or geographical location.	Yes	No	<code>DMZ Public</code>
<b>Start Address</b>	The start of the range of IP addresses that defines the zone.	Yes	No	<code>192.168.1.0</code>
<b>End Address</b>	The end of the range of IP addresses that defines the zone.	Yes	No	<code>192.168.1.255</code>
<b>Dynamic</b>	Determines whether the devices defined in the zone use dynamic addressing: <ul style="list-style-type: none"> <li><b>true</b>—devices in the zone use dynamic addressing (DHCP)</li> <li><b>false</b>—devices in the zone use static IP addressing</li> </ul>	No Default is <code>false</code>	No	<code>false</code>
<b>Category URI</b>	The asset category to assign to zone.  <b>NOTE:</b> The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes  This column can be repeated because a zone can be categorized into more than one asset category.	<code>/All Asset Categories/All Site Asset Categories/Business Impact Analysis/Business Role/Service/Web/</code>
<b>Ignore</b>	The column contains data that is not used by the Network Model wizard when creating zones. For example, this column could contain a description of the zone.	No	Yes	<code>This zone defines the public subnet of the DMZ.</code>

## Assets CSV File Format

Assets represent individual nodes on the network, such as servers and routers. For more information, see [“Understanding ESM Asset Resources” on page 95](#).

You can define a set of assets in ArcSight ESM by batch loading asset definitions from an Assets CSV file. Asset CSV files contain the columns listed in [Table 4-2 on page 102](#).

When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 104](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 97](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset data is imported into the ArcSight ESM Manager. The new assets are created in the `/All`

[Assets/Site Assets](#) group. For example, if an asset called `DMZCorpEmailServer` was specified in the imported assets CSV file, a new asset is created at the following URI: `/All Assets/Site Assets/DMZCorpEmailServer`. When imported, the new assets are auto-zoned. For more information, see [“Auto-zoning of Imported Assets” on page 105](#).

**Table 4-2 Assets CSV File Format**

Column Type	Description	Required Column?	Repeatable Column?	Example Value
<b>Name</b>	A descriptive name for the asset. This name must be unique. It is recommended to specify a name. However, if a name is not specified, a unique name is generated using the other fields.	No	No	<code>DMZ Corp Email Server 1</code>
<b>Host Name</b>	The host name of the network device represented by the asset.	No	No	<code>dmz_corp_eml1</code>
<b>IP Address</b>	The IP address of the network device represented by the asset.  <b>NOTE:</b> If no value is specified for this column (,) the asset is created with an IP address of <code>0.0.0.0</code> .	Yes	No	<code>192.168.2.1</code>
<b>MAC Address</b>	The MAC address of the network device represented by the asset. The MAC address is made up of six groups of two hexadecimal digits can be separated by colons (:) or hyphens (-).	No	No	<code>21-4D-5B-2A-3B-FF</code>
<b>Static Addressing</b>	Defines if the network device is statically addressed even though the IP address of the asset is in a dynamic zone:  <ul style="list-style-type: none"> <li><b>true</b>—asset uses static IP addressing</li> <li><b>false</b>—device uses dynamic addressing (DHCP)</li> </ul> For more information, see <a href="#">“Static Addressing in a Dynamic Zone” on page 103</a> .	No  Default is <code>false</code>	No	<code>false</code>

Column Type	Description	Required Column?	Repeatable Column?	Example Value
<b>Category URI</b>	The asset category to assign to network device. <b>NOTE:</b> The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes  This column can be repeated because a network device can be categorized into more than one asset category.	<a href="#">/All Asset Categories/Site Asset Categories/Business Impact Analysis/Network Domains/Email/</a>
<b>Ignore</b>	The column contains data that is not used by the Network Model wizard when creating assets. For example, this column could contain a description of the asset.	No	Yes	<a href="#">This asset defines the Corporate Email Server in the DMZ.</a>

### Static Addressing in a Dynamic Zone

Set the **Static Addressing** column to [true](#) if the network device is statically addressed even though the IP address of the asset is in a dynamic zone. For example, set this column to [true](#), for the following conditions:

- A dynamic zone is defined with the following IP range: [192.168.2.1 - 192.168.2.255](#).
- A network device with an IP address of [192.168.2.15](#) is statically addressed even though it is defined in the dynamic zone.

### Asset Ranges CSV File Format

**Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have a number of network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. An asset range can define a group of assets that are not addressed individually. Asset ranges should be a subset of the IP address ranges defined for zones.



Each asset range should specify a unique range of IP addresses. The IP addresses specified by asset ranges should not overlap. If you import an asset range that overlaps with an asset range already specified on the ArcSight ESM Manager and the new asset range has a different name than the existing asset range, the following occurs:

- the new asset range is created
- the existing asset range is invalid and displays with the broken asset range icon in the ArcSight ESM Console

You can define a set of asset ranges in ArcSight ESM by batch loading asset range definitions from an asset range CSV file. Asset range CSV files contain the columns listed in [Table 4-3 on page 104](#). When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Ranges Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 104](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 97](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset range data is imported into the ArcSight ESM Manager. The new asset ranges are created in the [/All Assets/Site Assets](#) group. For example, if an asset range called [DMZCorpHR](#) was specified in the imported asset range CSV file, a new asset range is created at the following URI: [/All Assets/Site Assets/DMZCorpHR](#).

**Table 4-3 Asset Ranges CSV File Format**

Column Type	Description	Required Column?	Repeatable Column?	Example Value
<b>Name</b>	A descriptive name for the asset range. This name must be unique.	Yes	No	<a href="#">DMZ Corp HR</a>
<b>Start Address</b>	The start of the range of IP addresses that defines the asset range.	Yes	No	<a href="#">192.168.2.11</a>
<b>End Address</b>	The end of the range of IP addresses that defines the asset range.	Yes	No	<a href="#">192.168.2.20</a>
<b>Category URI</b>	The asset category to assign to asset range.  <b>NOTE:</b> The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes  This column can be repeated because an asset range can be categorized into more than one asset category.	<a href="#">/All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/HR Data/</a>
<b>Ignore</b>	The column contains data that is <b>not</b> used by the Network Model wizard when creating asset ranges. For example, this column could contain a description of the asset range.	No	Yes	<a href="#">This asset range defines the all the corporate human resources assets.</a>

## Increasing the Number of Rows Displayed

By default, only the first fifteen rows of data are displayed in Select Column Headers for the <Resource Type> Data panels. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported.

To increase the number of rows displayed, add the property [usecase.networkmodeling.maxrowfortable](#) to the [<ARCSIGHT\\_HOME>/config/console.properties](#) file and set the value of the property to a number greater than fifteen. Restart the ArcSight ESM Console.



## Summary of Data to Import

In the Summary of Data to Import panel, a summary of the network modeling data ready to import into the ArcSight ESM Manager is displayed. If you click **Cancel** in this panel or any of the preceding panels, no data is imported into the ArcSight ESM Manager.

- 1 Click **Next** to start the import process.

A temporary Archive Resource Bundle (ARB) file with the import data is created and the Install Packages dialog displays.

- 2 To install the data from the temporary ARB file, in the Update Packages dialog, click **OK**.

The network modeling data is imported into the ArcSight ESM Manager and the Data Imported pane displays. In addition, the Installing Packages and the Importing Packages dialogs display.

- 3 Close the open dialogs:

- a In the Installing Packages dialog, click **OK**.
- b In the Importing Packages dialog, click **OK**.

## Network Data Imported into Manager

When network modeling data is imported from the network modeling data CSV files, new resources are created in the following groups on the ArcSight ESM Manager:

- New **zones** are created in the [/All Zones/Site Zones](#) group. For example, if a zone called [DMZPublic](#) was specified in the imported zones CSV file, a new zone is created at the following URI: [/All Zones/Site Zones/DMZ Public](#).  
The new zones are assigned to the default network called [Local](#).
- New **assets** are created in the [/All Assets/Site Assets](#) group. For example, if an asset called [DMZCorpEmailServer](#) was specified in the imported assets CSV file, a new asset is created at the following URI: [/All Assets/Site Assets/DMZCorpEmailServer](#). When imported, the new assets are auto-zoned. For more information, see [“Auto-zoning of Imported Assets” on page 105](#).
- New **asset ranges** are created in the [/All Assets/Site Assets](#) group. For example, if an asset range called [DMZCorpHR](#) was specified in the imported asset range CSV file, a new asset range is created at the following URI: [/All Assets/Site Assets/DMZCorpHR](#).

In the Data Imported dialog, click **Finish** to close the wizard.

## Auto-zoning of Imported Assets

When new assets are imported into the ArcSight ESM Manager using the Network Model wizard, an attempt is made to assign the assets to the appropriate zone from the default network called [Local](#). This process is called auto-zoning.

When the asset is imported, if a zone is found with an address range that includes the imported asset and that zone is located in the [Local](#) network, the matching zone is assigned to the asset. For the asset to find the matching zone, the matching zone must either:

- Already exists on the ArcSight ESM Manager prior to the import.
- Be imported with the asset as part of the same import process—part of the same transaction. Zones are created before assets in the import process.

If no matching zone is found in the network, no zone is assigned.

The following example illustrates the auto-zone process. A zone called **DMZCorporate** is defined in the **Local** network on the ArcSight ESM Manager with a starting address of **192.168.2.0** and an ending address of **192.168.2.225**. If an asset called **DMZCorpDatabase** with an IP address of **192.168.2.11** is imported by the wizard, the **DMZCorporate** zone is assigned to **DMZCorpDatabase** asset because the IP address of the **DMZCorpDatabase** asset is in the range of addresses specified in the **DMZCorporate** zone and the **DMZCorporate** zone is located in the **Local** network.



Only one asset with a given host name is allowed in a given zone on a network. When two assets with the same host name are imported, and if the ArcSight ESM Manager assigns them to the same zone in the same network, both assets are imported but one of the assets is disabled and displays with the broken-asset icon in the ArcSight ESM Console.

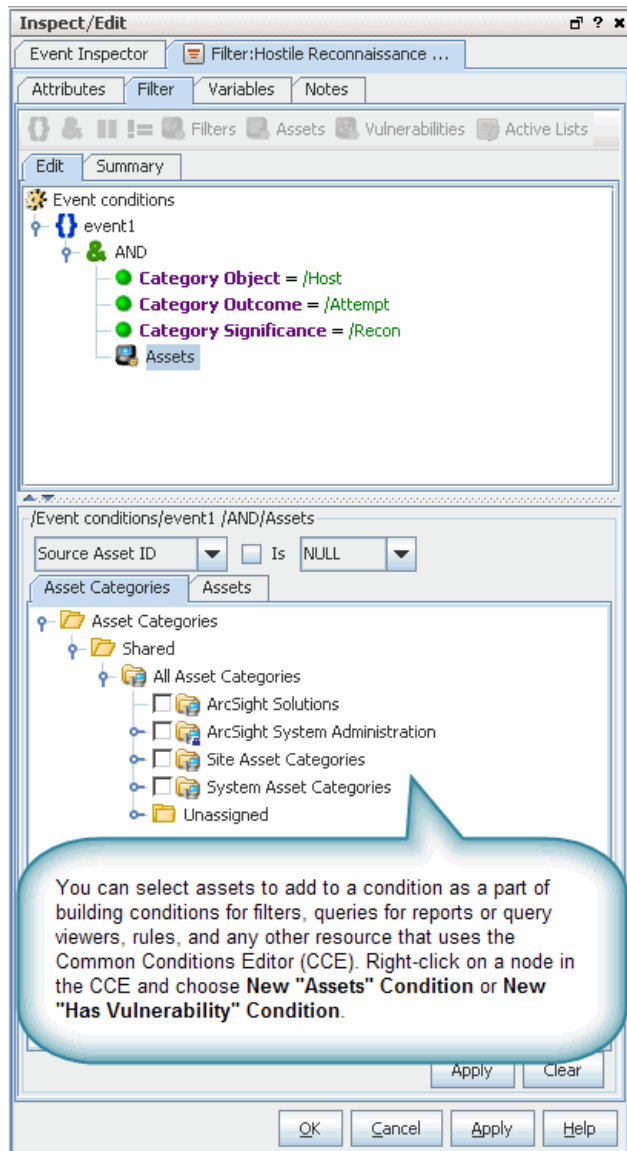
---

## Selecting Assets in the Common Conditions Editor

Once assets are added to your network model, you can select them in order to write conditions that help you analyze their role in the event traffic they process.

The Asset Selector appears in the Query Editor (in Reports), Rules Editor, Filters Editor, and in the Filter Settings panel, when creating an asset condition. In the Asset Selector, select the assets to add as a new condition.

Right-click on a node in the Common Conditions Editor (CCE) and choose **New "Assets" Condition**. (For more about using the CCE, the ESM User's Guide or Console Help.)



## Managing Assets

This topic explains how to create, edit, move, add to, and delete assets. Before making assets changes, however, please first see the overview in ["Understanding ESM Asset Resources"](#) on page 95.

## Creating an Asset

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 Right-click a group and choose **New Asset**.
- 3 Select the **Attributes** tab and enter values in the fields described below.
- 4 Click **OK**.

**Table 4-4 Asset Attribute Fields**

Asset Attributes	Description
Name	The asset's friendly name. This field can default to the asset's host name or IP address.
IP Address	The asset's IP address, in dotted-decimal notation.
MAC Address	The unique hardware ID for the network device.
Host Name	The asset's DNS name.
Location	As described in Assets and Changing Assets.
Zone	As described in Assets and Changing Assets.

After you fill in the attribute fields, use the other tabs in the Asset Editor as necessary to add resources.

**Table 4-5 Additional Asset Editor Tabs**

Asset View	Contents
Categories	Use the Add button on this tab to select network categories with which to associate the asset.
Alternate Interfaces	Use the Add button on this tab to select a second asset ID if this asset has an additional ID on another network. Alternate interfaces usually apply only to network boundary devices, such as bridges, that have two MACs.
Vulnerabilities	Use the Add button on this tab to select certain vulnerabilities with which to associate the asset.
Notes	Use the text box and Save button on this tab to write and file additional information concerning the asset.

## Working with Locations, Zones, Networks, Vulnerabilities, and Categories

As a part of identifying assets and configuring ESM to recognize them, you need to provide detail about networks, zones, and locations where assets reside. Additionally, you can list vulnerabilities separately, and group assets into categories based on which you can set up user access controls and monitoring channels.

You can create and edit descriptions of networks, zones, locations, and particular assets considered to be *vulnerabilities*. Editors for these are provided as right-click options on the resources in the Assets subtabs for Networks, Zones, Locations, Vulnerabilities. Each has

slightly different attributes and configuration information on sub-tabs, depending on the type of asset resource.

## Location Editor

Asset Attributes	Description
Name	A descriptive name for the geographical location (required)
Latitude	Latitude for the location.  The format for this measurement is a preference setting for the Console (menu option <b>Edit &gt; Preferences</b> , click Latitude and Longitude). For more information, see <a href="#">"Latitude and Longitude Options" on page 561</a> in <a href="#">"Changing User Preferences" on page 556</a> .
Longitude	Longitude for the location  The format for this measurement is a preference setting for the Console (menu option <b>Edit &gt; Preferences</b> , click Latitude and Longitude). For more information, see <a href="#">"Latitude and Longitude Options" on page 561</a> in <a href="#">"Changing User Preferences" on page 556</a> .
Address	Provide details for <b>City</b> , <b>Region Code</b> , <b>Postal Code</b> , and <b>Country</b>

## Zone Editor

Asset Attributes	Description
Name	A descriptive name for the geographical location (required)
Start Address	Provide an IP address that identifies the start of the network scope.
End Address	Provide an IP address that identifies the end of the network scope.
Dynamic Addressing	Click this option on or off to indicate whether this network uses dynamic addressing <ul style="list-style-type: none"> <li>• Checkmark (toggle <b>on</b>) this option to indicate that the network you are describing <b>uses dynamic addressing</b> (Dynamic Host Configuration Protocol or DHCP server)</li> <li>• Leave this option unchecked (toggle <b>off</b>), if the network you are describing does not use dynamic addressing (but, rather, <b>uses static IP addresses</b>)</li> </ul>
Location	Select a location for this zone.
Network	Select the network in which this zone resides.

In addition to zone **Attributes** (described above), the Zone Editor includes subtabs for adding **Assets** and **Categories** into the *zone* you are configuring.

## Network Editor

Asset Attributes	Description
Name	A descriptive name for the network (required)
Customer	Customer name  This option is typically used if configuring assets for a customer on behalf of a managed security service provider (MSSP) or similar scenario.
Location	This is an optional field for a descriptive name of the geographical location of the network.

In addition to network **Attributes** (described above), the Network Editor includes subtabs for adding **Connectors** and **Zones** into the selected *network* you are configuring.

## Vulnerability Editor

Asset Attributes	Description
Name	A descriptive name for the vulnerable asset (required)
Knowledge Base Article	Optionally, provide a link to a relevant knowledge base article.
External ID	Provide an alternate identifier for the vulnerability.

In addition to vulnerability **Attributes** (described above), the Vulnerability Editor includes a subtab for selecting and adding assets as **vulnerabilities**.

## Categories

The Asset Categories subtab in the Navigator provides options to organize assets into groups based on *categories*. From the Navigator right-click menu on Asset Categories, you have several views and tools to help manage and monitor assets. For example, from this menu, you can:

- Create channels to show asset categories and assets
- Move assets into and out of category groups
- Create new category groups
- Configure access control lists (ACLs) to limit or allow user access to groups of assets (see [“Managing Permissions and Resources” on page 81](#))

One asset can be categorized in more than one asset category. You can also assign asset categories to groups of resources. This transfers the asset category onto all the members of the group and its sub-groups. To assign an asset category:

- 1 In the Navigator drop-down menu, go to **Assets**. Select the **Assets** tab. Go to [ArcSight System Administration/Agents](#), where you will find the SmartConnectors installed for your environment.
- 2 Right-click the asset or asset group you wish to categorize and select **Edit Asset** (or **Edit Group**).

- 3 In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen.
- 4 In the Asset Categories Selector pop-up window, select the asset categories that apply to this asset and click **OK**. For example:
  - a The usage category that applies to the asset (for example, /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation)
  - b The criticality level that applies to the asset (for example, /All Asset Categories/System Asset Categories/Criticality/Very High)
- 5 Repeat steps 3 and 4 for every asset or group of assets you wish to classify in one of the ESM asset categories.

For more information about asset categorization and categories in ESM, see the ESM User's Guide or Console Help.

## Editing an Asset

- 1 In the Assets resource tree, right-click an asset and choose **Edit Asset**.
- 2 On the **Attributes** tab, edit the text fields as described above.
- 3 On the other tabs, add or delete information as necessary.
- 4 Click **OK**.

## Moving or Copying an Asset

- 1 In the Assets resource tree, navigate to an asset and drag and drop it into another group.
- 2 Choose **Move** to move the asset, **Copy** to make a separate copy of the asset, or **Link** to create a copy of the asset that is linked to the original asset.

If you choose **Copy**, you create a separate copy of the asset that will not be affected when the original asset is edited. If you choose **Link**, you create a copy of the asset that is linked to the original asset. Therefore, if you edit a linked asset, whether the original or the copy, all links are edited as well. When deleting linked assets, you can either delete the selected asset or all linked asset copies.

## Deleting an Asset



Never delete System Asset resources of any type without consulting an ArcSight administrator. System Asset resources are usually necessary for correct operation.

- 1 In the Assets resource tree, right-click an asset and choose **Delete Asset**.
- 2 In the dialog box, click **Yes**.

## Showing Assets in a Channel

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Show Assets**.

The asset(s) are displayed in an active channel grid view.

- 2 If applicable, you can also show assets recursively. To do so, right-click an asset group, and choose **Show Assets Recursively**. This will show assets not only in the selected group but also all children in an active channel.

## Auto Zoning an Asset

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Auto Zone**.

The Network Selector dialog displays.

- 2 Browse for the network that contains the zone with an IP address range that includes the asset.
- 3 Select the network and click **OK**.

If a matching zone with an address range that includes the selected asset can be found in the network, the zone is assigned to the asset. For example, a zone called **DMZCorporate** is defined in the **Local** network on the ArcSight ESM Manager with a starting address of **192.168.2.0** and an ending address of **192.168.2.225**. If an asset called **DMZCorpDatabase** with an IP address of **192.168.2.11** is selected for auto zoning in the **Local** network, the **DMZCorporate** zone is assigned to **DMZCorpDatabase** asset because the IP address of the **DMZCorpDatabase** asset is in the range of addresses specified in the **DMZCorporate** zone.

If no matching zone is found in the network, no zone is assigned.

An asset can be selected for auto zoning manually by right-clicking and choosing the **Auto Zone** option as described above. In addition, auto zoning can automatically occur when assets are imported using the Network Model wizard. For more information, see ["Auto-zoning of Imported Assets" on page 105](#).

## Managing Asset Groups

Asset groups are created to store similar groups or assets in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's permissions. If a group is deleted, the assets within that group are also deleted. ArcSight provides these groups:

- **Shared**: this group lists assets to which the user has permission.
- **Unassigned**: this group lists assets not assigned to a group.

If you have Administrator access you will also see another group named "All Assets" that contains all asset groups and assets.

## Creating an Asset Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 In the Assets resource tree, right-click a group and choose **New Group**. A "name" text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

## Renaming an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

## Editing an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Edit Group**.



- 2 In the **Group Editor**, edit the Name and Description text fields.
- 3 Click **OK**.

## Moving or Copying an Asset Group

- 1 In the Assets resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

## Deleting an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

## Asset Scalability

ArcSight stores information about hosts and network devices in resources called Assets. These resources can be automatically created by vulnerability scanner SmartConnectors. Asset Scalability refers to ArcSight's ability to manage hundreds of thousands of assets or more without adversely affecting security event throughput.

## Viewing Assets in Active Channels

Starting with ArcSight ESM v4.0, the Console shows assets, vulnerabilities, asset categories, scanner reports, and cases in active channels (rather than static grid views, as in previous releases). Now you can leverage the power of channels for asset management, including use of filters, field sets, better sorting capabilities, and dynamic display of an unlimited number of items (continually updated).

To start working with assets in active channels, choose **Assets** in the Navigator, and see [“Modeling Your Network and Managing Assets” on page 93](#).

Note also that you can create an “asset channel”. For more information on active channels, see the ESM User's Guide or Console Help.

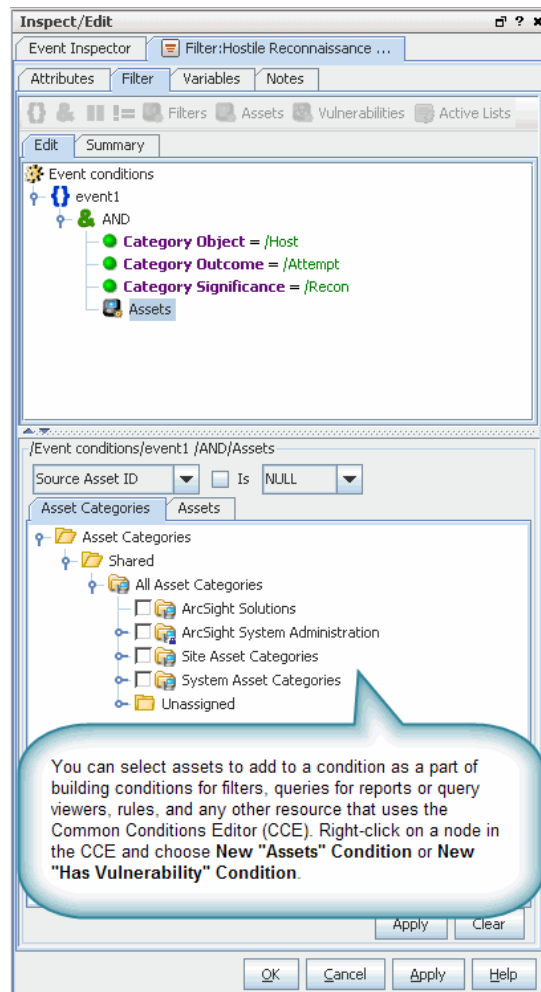
## Finding Assets

Resource search helps you find one asset in a potentially large set, avoiding the resource tree in the Navigator.

## Selecting Vulnerabilities

You can open the Vulnerability Selector from the Reports Query Editor, Rules Editor, Filters Editor, and in the Filter Settings panel. In the Vulnerability Selector, you select vulnerabilities to add to reports, rules, or filters as a new condition.

Right-click on a node in the Common Conditions Editor (CCE) and choose **New "Has Vulnerability" Condition**. (For more about using the CCE, see the ESM User's Guide or Console Help.)



You use the Vulnerability Selector when performing these tasks:

- Adding a vulnerability condition to a report query (see the “Query Conditions” topic in the ESM User's Guide or Console Help)
- Specifying rule conditions (see the ESM User's Guide or Console Help)
- Using filters (see [“Using Filters” on page 118](#))

## Managing Vulnerabilities

This topic describes how to perform the authoring and management tasks for vulnerabilities. See also [“Modeling Your Network and Managing Assets” on page 93](#).

Note also that you can create a “vulnerability channels”. For more information on active channels, see the ESM User's Guide or Console Help.

### Creating a Vulnerability

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.

- 2 Right-click a group and choose **New Vulnerability**.
- 3 On the Vulnerabilities Attributes tab, type in the following text fields:

Vulnerability Attribute	Description
Name	The vulnerability's name. It can be generated by the ArcSight Manager in response to vulnerability scanners. If so, this field will be identical to the <b>External ID</b> field except that the pipe ( ) will be replaced with a dash (-), such as CVE - CVE-1999-200.
Knowledge Base Article	A Knowledge Base article that further describes the vulnerability.
External ID	An ID of the format <standards body> <id>, such as CVE   CVE-1999-200.
Owners	ArcSight users who are interested in the vulnerability.
Notification Groups	ArcSight users who are notified of events involving the vulnerability.

- 4 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 5 Click **OK**.

## Editing a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 On the Attributes tab, type in the text fields as described above.
- 3 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 4 Click **OK**.

## Moving or Copying a Vulnerability


- 1 In the Vulnerabilities tree, navigate to a vulnerability and drag and drop it into another group.
- 2 Choose **Move** to move the vulnerability, **Copy** to make a separate copy of the vulnerability, or **Link** to create a copy of the vulnerability that is linked to the original vulnerability.

If you choose **Copy**, you create a separate copy of the vulnerability that will not be affected when the original vulnerability is edited. If you choose **Link**, you create a copy of the vulnerability that is linked to the original vulnerability. Therefore, if you edit a linked vulnerability, whether it be the original or the copy, all links are edited as well. When deleting linked vulnerabilities, you can either delete the selected vulnerability or all linked vulnerability copies.


## Retrieving Vulnerable Assets

- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 Select the **Vulnerable Assets** tab.


If you used a vulnerability scanner, all vulnerable asset discovered by the scanner are listed on this tab.

- 3 To refresh the vulnerabilities list, click the **Refresh** button (  ).

## Adding an Asset to a Vulnerability

- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Click the **Add** button (  ).
- 4 Select an asset in the Assets Selector and click **OK**.
- 5 In the Vulnerability Editor, click **OK**.

## Deleting an Asset From a Vulnerability

- 1 In the Vulnerabilities tree, right-click an asset and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Select an asset and click the **Delete** button (  ).
- 4 In the dialog box, click **Yes**.
- 5 In the Vulnerability Editor, click **OK**.

## Deleting a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Delete Vulnerability**.
- 2 In the dialog box, click **Yes**.

## Managing Vulnerability Groups

This topic describes the tasks involved in managing vulnerability groups.

### Creating a Vulnerability Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then the **Vulnerabilities** tab.
- 2 In the Vulnerabilities resource tree, right-click a group and choose **New Group**.  
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

### Renaming a Vulnerability Group

- 1 In the Vulnerabilities resource tree, under Assets, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

### Editing a Vulnerability Group

- 1 In the Asset resource tree's Vulnerabilities tab, right-click a group and choose **Edit Group**.

- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

## Moving or Copying a Vulnerability Group

- 1 In the Vulnerabilities tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

## Deleting a Vulnerability Group

- 1 In the Vulnerabilities tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

## Reporting on Scanners

You can conveniently review the output of asset-vulnerability scanners in active channels and in the Vulnerabilities tab of the Asset Editor.

- 1 Choose the Assets resource tree in the Navigator panel.
- 2 In the Assets tab of the Assets tree, right-click an individual asset and choose **Scanner Reports**. If scanner asset-vulnerability reports are available for the selected asset, they appear in a Viewer panel grid view as an active channel.
- 3 You can use the standard controls described in Using Grids and Active Channels to review the reports collectively.
- 4 Also in the channel view, you can double-click vulnerability scanner events to open them in the Asset Editor, where the Vulnerabilities tab lists the vulnerability details.

For information on creating and editing assets, see [“Modeling Your Network and Managing Assets” on page 93](#).

You can create an active channel for selected scanner reports. For information on using active channels, see the ESM User's Guide or Console Help.

## Reporting Vulnerable Assets

You can create reports to show which assets are vulnerable to particular vulnerabilities or threats. ArcSight also provides Asset Reports that can be run from the Reports resource tree in the Navigator panel. For more information, see the ESM User's Guide or Console Help.

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.
- 2 In the Vulnerabilities tree, right-click a vulnerability and choose **Vulnerable Assets Report**.

- 3 In the Report Parameters dialog box, accept the vulnerability listed in the **Vulnerability URL** text field or click the **Vulnerability** button to run the report on another vulnerability.
- 4 Choose a Report File Format from the drop-down menu.
- 5 Click **OK**.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and will appear differently. In addition, Excel format is more memory intensive than PDF.

## Managing Filters

The Filters resource tree in the Navigator panel is pre-populated with some typical event filters you can use directly, or as templates for more specific purposes.

### Using Filters

The maintenance tasks for filters include editing, moving, copying, importing, exporting, and deleting. (Tasks described here are considered administrator tasks. For information on using filters, see also “Filtering Events” in the ESM User’s Guide or Console Help.)

### Editing a Filter



Understanding how to use the Common Conditions Editor (CCE) is integral to creating and editing filters. (For more information, see the ESM User’s Guide or Console Help.)

---

- 1 In the Filters resource tree, right-click a filter and choose **Edit Filter**.
- 2 In the Filters Editor, edit the filter name.
- 3 In the conditions editor, edit logical operators and condition statements by doing the following:
  - ◆ To edit a logical operator, right-click the logical operator and choose **Edit**, then choose a logical operator and click **OK**. (For more information, see the ESM User’s Guide or Console Help.)
  - ◆ To edit a condition statement, right-click the condition statement and choose an operator, condition editor, or selection operation. (For more information, see the ESM User’s Guide or Console Help.)
  - ◆ To delete a logical operator, right-click the operator and choose **Delete**. In the confirmation dialog box, click **Yes**. The logical operator and all its condition statements are removed.
  - ◆ To delete a condition statement, right-click it and choose **Delete**. In the confirmation dialog box, click **Yes**.
  - ◆ To edit or delete a filter, right-click the filter and choose **Edit** or **Delete**.
- 4 Click **OK**.

## Importing and Exporting filters



To import and export filters, use the packages feature. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. For more information on packages, see [“Managing Packages” on page 129](#).

For information on how to import and export filters on SmartConnectors, see [“Importing and Exporting SmartConnector Configurations” on page 164](#) (especially the topics on [“Creating SmartConnector Filters” on page 152](#) and [“Adding SmartConnector Filter Conditions” on page 153](#)).

## Moving or Copying Filters

- 1 In the Filters resource tree, navigate to a filter and drag and drop it into another group.
- 2 Choose **Move** to move the filter, **Copy** to make a separate copy of the filter, or **Link** to create a copy of the filter that is linked to the original filter.

If you choose **Copy**, you create a separate copy of the filter that will not be affected when the original filter is edited. If you choose **Link**, you create a copy of the filter that is linked to the original filter. Therefore, if you edit a linked filter, whether it be the original or the copy, all links are edited as well. When deleting linked filters, you can either delete the selected filter or all linked filter copies.

## Deleting Filters

- 1 In the Filters resource tree, right-click a filter and choose **Delete filter**.
- 2 In the dialog box, click **Yes**.

## Using Filter Groups

Filter groups are created to store similar groups or filters in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's access control list (ACL).

Groups and filters can be managed with drag and drop functionality. You can move or copy groups and filters into other groups. If a group is deleted, the filters within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

## Creating Filter Groups

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a group and choose **New Group**.
- 3 In the Name text field, type in a name.
- 4 Press **Enter**.

## Renaming Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.

- 2 In the Name text field, rename the group.
- 3 Press **Enter** and click **OK**.

## Editing Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields, and press **Enter** after each.
- 3 Click **OK**.

## Moving or Copying Filter Groups

- 1 In the Filters resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.


If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.


## Deleting Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

# Managing Notifications

## Managing Received Notifications

When the Notifications button in the Console toolbar indicates that new notifications have arrived (  ), you click that button to open the Notifications tab in the Viewer panel. This is your central notification repository.

You can open the Notifications manager at any time by clicking the toolbar button, even if no new notifications are present (  ).


To use the Notifications manager you first choose a category tab for the type of notification received.

Notification Category	Use
Pending	These are notifications that you have not yet handled (reassigned to one of the following categories). Pending notifications older than 24 hours are automatically refiled as Not Acknowledged.
Undelivered	These are notifications that were not delivered.
Acknowledged	These are notifications to which you have replied.
Not Acknowledged	Pending notifications that go unacknowledged or unresolved for more than 24 hours are automatically refiled as Not Acknowledged.



Notification Category	Use
Resolved	These are notifications for which you or a colleague have found a resolution and so have marked the notification accordingly.
Informational	These are notifications that are provided for information purposes only and do not require resolution or intervention.

---




If you don't see notifications appearing, make sure your ArcSight user identity (not just your e-mail address) is set as a destination in the Notifications Editor.

In a category, click **Acknowledge** to mark a selected notification as acknowledged. Click **View Event** to see the event that triggered a notification. Click **Resolve** to reclassify the notification as Resolved.

For each category of notification there is a common set of columns of information concerning them..

Notification Column	Definition
Priority	This is the same priority set by the SmartConnector and modified by the current threat level formula (and seen in grid views), unless modified by the rule that triggered the notification.
Triggering Event	The event that caused the rule to trigger the notification.
Notification Group	The branch of the Notifications resource tree to which this destination belongs.
Escalation Level	The Escalation Level (and implied destinations) the notification has reached while waiting for resolution.
Create Time	The time at which the notification was created

---



Also note that you can set a severity threshold for notification pop-ups and sounds in Console Preferences, and also manage your notifications from an ArcSight Web browser client.

## Managing Notification Groups and Levels

This chapter describes how to handle the tasks required for managing notification groups and levels.

### Creating Notification Groups

- 1 On the Navigator panel drop-down menu, choose the **Notification** resource tree.
- 2 In the Notification panel, right-click **All Destinations** and choose **New Group**.  
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.

- 4 Press **Enter**.



As a user, you can create new groups under **All Destinations**, but not new subgroups under existing system-defined groups.

---

## Renaming Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

## Editing Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

## Deleting Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

## Adding Escalation Levels

In the **Notifications** resource tree, right-click a notification group and choose **Add Escalation Level**.

New escalation levels are added in sequential order. If you want to add a level between two existing levels, add another level then move destinations accordingly. For example, if you have **Level 1** and **Level 2** and you want to add a level between them, add another level, **Level 3**. Then, move all destinations from **Level 2** to the new **Level 3**.

## Deleting Escalation Levels

- 1 In the **Notifications** resource tree, select the last escalation level in a notification group.



All destinations within this escalation level will also be deleted. If you want to save the destinations, make sure you move them to another level **before** deleting.

---

- 2 Right-click the escalation level and choose **Delete Escalation Level**.

## Managing Notification Destinations

The task descriptions in this topic explain how to manage notification destinations.

### Creating Destinations

- 1 In the **Notification** resource tree in the **Navigator** panel, right-click an escalation level (such as **Level 1**) and choose **Add New Destination**.
- 2 In the **Notification Editor**, enter a label for the notification in the **Name** field.
- 3 Set a **Start Time** and **End Time** during the day within which the notification will be active. The default is all day (12:00:00 AM to 11:59:59 PM).

- 4 For destinations other than the ArcSight Console, select that **Destination Type** and enter the **Address**, **PIN**, or **Provider** for that device.
- 5 For the ArcSight Console, choose a **User/Group** identity.



Always set the ArcSight **User/Group** identity. If not set, notifications cannot be sent to users' Consoles.

- 6 Click **OK**.

## Editing Destinations

- 1 In the Notification resources tree, right-click a notification destination and choose **Edit Destination**.
- 2 In the Notification Editor, edit the Value fields for the necessary destination attributes.
- 3 Click **OK**.

For more information, see [“Changing Notification and Acknowledgement Settings” on page 123](#).

## Moving or Copying Destinations

- 1 In the Notification resources tree, find a destination and drag it to a different escalation level. You can drag across groups if needed.
- 2 Right-click the destination and choose **Move** to move it, **Copy** to make a separate copy, or **Link** to create a copy of the destination that is linked to the original destination.

If you choose **Copy**, you create a separate copy of the destination that will not be affected when the original destination is edited. If you choose **Link**, you create a copy of the destination that is linked to the original destination. Therefore, if you edit a linked destination, whether the original or the copy, all links are edited as well. When deleting linked destinations, you can either delete the selected destination or all linked destination copies.

## Deleting Destinations

- 1 In the Notification resource tree, right-click a notification destination and choose **Delete Destination**.
- 2 In the dialog box, click **Yes**.

## Changing Notification and Acknowledgement Settings

Administrators can configure notifications, acknowledgements, and wait-time settings. The escalation time window or wait-time depends on the event's severity.



If notifications and/or acknowledgements were disabled during Manager setup, mail server settings made through the Console will not take effect until you re-run the Manager setup to enable notifications and/or acknowledgements on the Manager side.

To run the Manager setup: (1) stop the Console and Manager, (2) re-run the Manager setup wizard from the Manager's `/bin` directory ([arcsight managersetup](#)). See the *ArcSight ESM Installation and Configuration Guide* for more information.

## Changing E-mail Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit E-mail Settings**.
- 2 In the Notification Editor, type in the following text fields:

Notification Fields	Definition
From Address	The e-mail address from where the notification messages are sent. It is important that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses. For notifications sent by cell phone, any cell phone must be e-mail enabled.
Outgoing Mail Server	The host name of the local outgoing mail server. This is the SMTP server ArcSight uses to send e-mail. The Outgoing Mail Server must be accessible from the ArcSight Manager for e-mail notifications to be sent. SMTP is used to send e-mail. An SMTP server must be configured either at install time or set here.
Incoming Mail Server	The local incoming mail server host name.
Incoming Mail Protocol	Select either IMAP or POP3 mail protocols.
E-mail Account	The e-mail account name. For notifications sent by e-mail, you need to add an address to the e-mail Address field.



POP3 and IMAP can be used to check for e-mail acknowledgments. You can specify these options at install time, or set them here. For acknowledgements, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

- 3 Type the **E-mail Account** password in the Password text field and confirm it in the Confirm **Password** text field.
- 4 Click **OK**.

## Adding New Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings**, **Edit Pager Providers**, then **New Service Provider**.
- 2 In the Notification Editor, type in the following text fields:

Pager Notification Field	Description
Provider Name	The name of the service provider, such as Skytel.
Host	The host name for the service provider's server, such as snpp.skytel.com. SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager provider host and port information.
Port	The port number for the service provider's server.

- 3 Click **OK**.



For notifications sent by pager, firewalls must be configured so that the pager can connect directly to the paging service provider. ArcSight currently supports any provider that supports SNPP.

## Editing Pager Service Provider Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, edit the text fields.
- 3 Click **OK**.

## Deleting Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, click **Delete**.

## Changing Wait Time Settings

The default wait-time values for Very-High severity is set for 2 minutes, High is set at 5 minutes, Medium is set for 30 minutes, and Low is set for 2 hours.

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit Escalation Wait Time**.
- 2 In the Notification Editor, type in the wait time for the hour (**Hr**) and minute (**Min**) text fields for **Very-High**, **High**, **Medium**, or **Low** severity.
- 3 Click **OK**.

## Testing Notification Groups and Destinations

This topic describes how to test notification groups and destinations.

### Testing Group Notifications

In the Notification resource tree, right-click a populated notification group and choose **Test Group Notification**.

A test notification message is sent to the notification destination. Test notifications are not sent to group notification destinations if the End Time has expired. For example, if you test group notification at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message will not be sent to the group.

### Testing Destination Notifications

In the Notification resource tree, right-click a notification destination and choose **Test Destination Notification**.

A test notification message is sent to the notification device. Test notifications are not sent to notification destinations if the End Time has expired. For example, if you test a notification destination at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message will not be sent to the device.

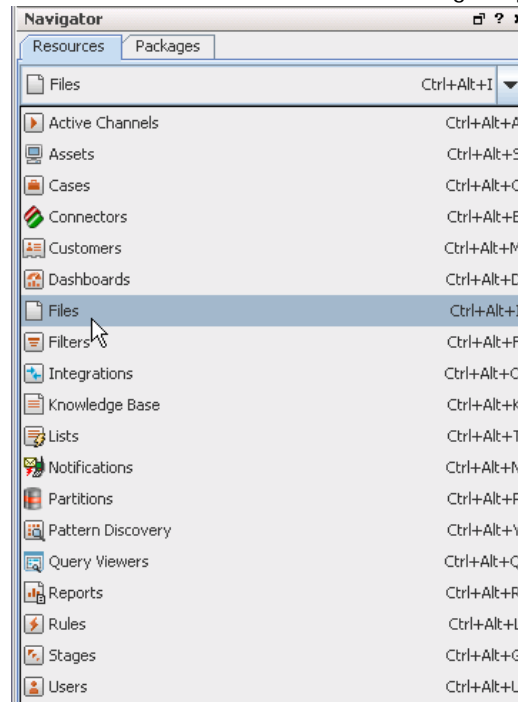
## Managing File Resources

The Files resource tree, when populated, lists various files that have been saved as resources so that they are accessible to all users of the system who are authorized for such access. File resources include Case file attachments, templates, and general-purpose shared files.

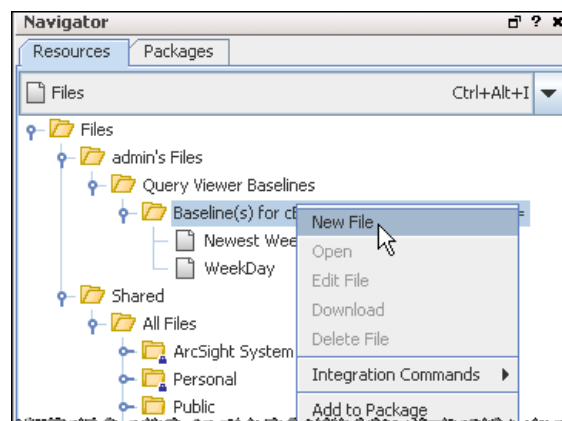
In addition to the tasks detailed below, you can also rename or lock a file, get a Graph View of a file, and so forth. Simply select the file in the Navigator, right-click, and choose a menu option. Operations on groups are also available. Options may vary depending on which file or folder you have selected in the Navigator.

## Uploading Files and Creating a File Resource

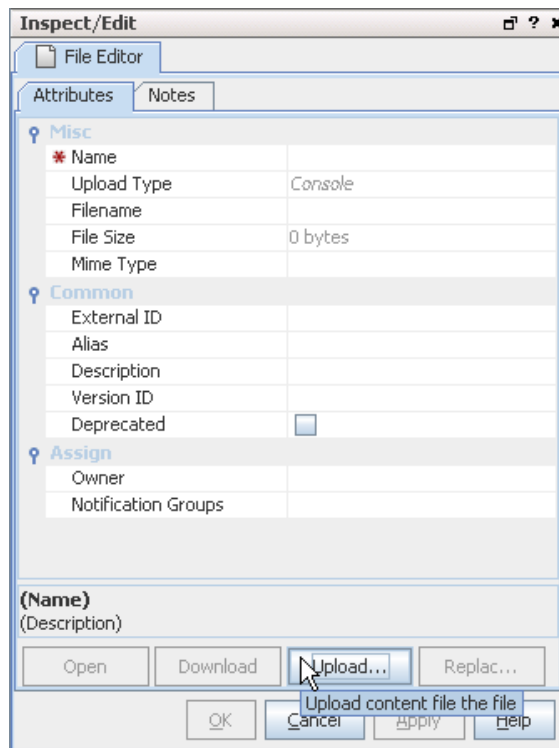
- 1 Choose the **Files** resource tree in the Navigator panel.



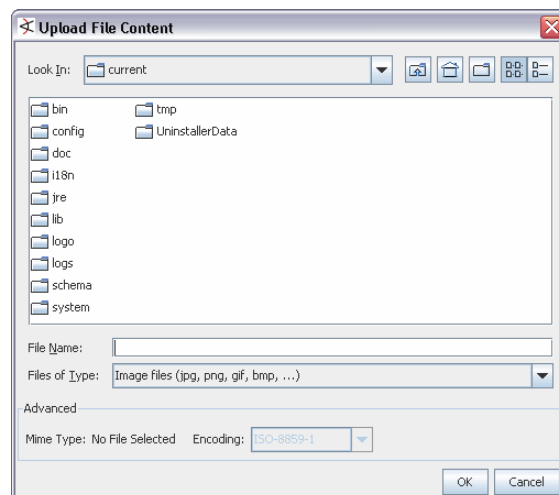
- 2 Right-click a file group and choose **New File**.



This brings up the File Editor in the Inspect/Edit panel.



- 3 Click the **Upload** button on the File Editor and select the local file to add.



- 4 On the File Editor Attributes tab, enter values for the attributes that identify the file.  
The Name attribute is initially the same as the Filename attribute, but you can change the Name.  
Certain attributes are read-only: Upload type is Console, and Filename, File size, and Mime type are set based on the selected file.
- 5 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

## Viewing Files

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Open**.
- 3 The file will be downloaded to a temporary directory (in a sub-directory called **arcsight-files**) and will launch in an appropriate viewer, usually a web browser.

You can also open a file resource from the File Editor by clicking the **Open** button.

## Downloading Files Locally

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Download**.
- 3 Specify a location and file name for the new local file.



File resources can be downloaded as often as needed by any console user authorized to access the file resources. Downloading a file does not change the file resource, or the shared file contents on the server.

---

You can also Download a file resource from the File Editor by clicking the Download button.

## Editing File Resource Attributes

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

## Replacing File Resource Contents

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Click **Replace** and select the local file containing the new contents for the file resource. The file resource name will change if the selected local file has a different name.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

## Deleting File Resources

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Delete File**.
- 3 Click **Yes** to confirm the deletion.

## Adding a File or Folder to a Package

From the Files resource Navigator, you can add a file or folder to an existing package or create a new package and add the file to it.



- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file or folder and choose **Add to Package**.  
This brings up the Package Selector dialog.
- 3 In the Package Selector dialog, do one of the following:
  - ◆ Navigate to a package to which you want to add the file or folder, and click **OK**. (The file is saved to the selected package.)
 Or
  - ◆ Navigate to a location where you want to create a new package and click **New Package**. (This brings up the Package Editor where you can name and configure the new package. The selected file or folder will be included in the new package.)

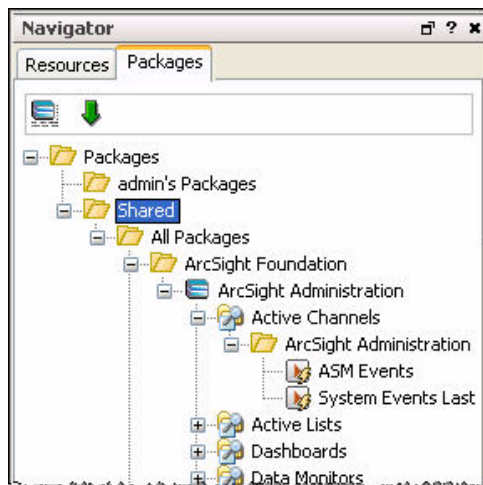
## Finding Files


To find files stored on the Manager, choose **Files** in the Navigator and browse the folders or choose **Edit > Search** from the menus, enter a file name in the **Search query** field, and click **Find**. (See ["Finding Resources" on page 171](#) for more information on this utility.)

For more information, see ["Managing Packages" on page 129](#).


## Managing Packages

Packages are collections of resources that can be installed into the system resource tree.



To access available packages, click the **Packages** tab of the Navigator panel. The tree of all packages is displayed along with the resources within each package. The  button toggles between Normal and Advanced view of the package tree. In the Advanced view, uninstalled packages are visible and package dependencies are shown.


## Viewing Installed Packages

Click the **Packages** tab in the Navigator panel. If the  button is highlighted, click it to return to Normal view. The tree view is like the tree view of any other resource except that the resources contained within packages may be of many different types.




The Packages tree view is independent of which resource you have selected in the Navigator. Regardless of which resource is selected, when you click on the **Packages** tab, you will see the same set of packages. These include the ArcSight stock content packages installed on the Manager along with any custom packages administrators have created on this Manager.

## Viewing all Packages (with Dependencies)

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view. In the Advanced view, all packages (including uninstalled packages) and package dependencies are shown.

## Showing Package Archive Contents

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view (to show all packages including uninstalled packages). Right-click a package and choose **Show Package Archive Contents** or **Show Current Package Archive Contents** (available only on installed packages). This lists all resources in the package, including details such as resource name, type, and full path to location in the tree.

## Creating Packages

- 1 Right-click the **Package Group** in the Packages tree that will contain the new Package. Choose **New Package**.
- 2 In the Package Editor that opens in the Inspect/Edit panel, enter the following fields

In this field...	...enter this
Name	Enter a name for the new package.
Required Packages	Specify the packages that must be installed for this package to function.
Optional Packages	Specify packages that are related to this package, but which are not required for it to function.
Required Features	Enter any ArcSight ESM features that must be available for this package to function. The pick list of features includes Pattern Discovery, for example.
Installed	(Read-only.) Check this box to indicate that the new package is installed. Unchecking this box is a good way to preview a new package before making its resources visible to all users of the system.
Update Available	(Read-only.) Check this box to indicate to other users that a newer version of the package exists.

In this field...	...enter this
Author Name	Enter the name of the author or source for the new package.
Package Version	The package version can be any string, but by convention, ArcSight recommends a format of 0.0.0.0, with numbers in decreasing importance (major, minor, release, build).
ArcSight Version	(Read-only.) The minimum ArcSight Version needed to support this package.
Format	<p>(Advanced) if you need a specific behavior, choose one of the choices other than default. Otherwise, leave this field set to default.</p> <p><b>Default</b> - Appropriate format for backing up resources on a Manager. This format captures more information than the other options, including information specific to a Manager installation.</p> <p><b>Export</b> - A portable format appropriate for packaging resources for transport between systems in which Manager-specific information is excluded from the exported package for resources with attributes that would otherwise retain such information upon a "default" export.</p> <p>For example, a trend packaged in "export" format does not include Start Time or End Time trend attributes nor original table IDs. Instead, the imported trend uses Start and End times that correspond to the time the package is installed on a new system. Also at time of package install, a new trend table is created. (See also, descriptions of Imported Trend Start Time and Imported Trend End Time fields under advanced Trend Attributes in "Building Trends" in the ESM User's Guide or Console Help.)</p> <p>Similarly, active lists and session lists packaged in "export" format do not include locked by attributes, table IDs, or session/active list entry attributes, respectively. New tables are created when the lists are imported, and the other attributes are tracked starting with launch of these resources on the new system.</p> <p>The package "export" format packages other resources similarly as a means of optimizing portability for content distribution.</p> <p>ArcSight system content is packaged using the "export" format. Also, Managed Service Security Providers (MSSPs) who provide content to ArcSight ESM installations at various customer sites might typically package resources in this format.</p> <p><b>Exportuser</b> - Highly portable format appropriate only for exporting user accounts with no permissions, personal group information, or relationships to other resources. If you want to export user accounts that include permissions and groups, use the default format instead.</p> <p><b>Upgrade</b> - For use by Arcsight Professional Services only. This format might be used for ArcSight initiated incremental resource upgrades of older systems in particular circumstances. (In most cases, standard upgrade utilities and processes are used instead.)</p>
Obfuscated	(Advanced) Check this box to scramble the package contents to prevent unauthorized viewing or modification.

In this field...	...enter this
Exclude Reference IDs	(Advanced) Check this box to remove reference IDs from the package when it is exported. Generally, you would exclude reference IDs only when you plan to import the package into a different ArcSight system. Leave the box unchecked to include reference IDs, which improve performance for packages that are imported to the same Manager from which they were exported.


**3** Click the **Resources** tab in the Package Editor. Click the **Add** drop-down menu to select the resources that this package will contain. You can select groups or individual resources.

Check the Children Only box to include resources below the specified resource in the tree. For example, selecting the group /All Session Lists/ArcSight Administration/User and checking Children Only would include only the session list resources in that group, not the group itself.

Check the Only If Referenced box to conditionally include resources if they are referenced by other resources without the Only If Referenced box checked.


**4** To exclude resources from the new package by resource type or by specifying actual resources to be removed, use the Removed Resources panel in the lower half of the Resources tab. To exclude resources by type, click the **Excluded Resource Types** tab and select from the list of available types. To exclude specific resources, click the **Removed Resources** tab, click the **Add** drop-down menu, then choose the resource(s) you wish to exclude using the resource picker.

---



The only way to exclude Asset Category resources from a package is to specify the Asset Categories explicitly using the Removed Resources tab.

## Importing Bundles

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Click the  icon to import a bundle.
- 3 Choose an .arb file to import and click **Open**.
- 4 Review the Import dialog for any conflicts. Each conflict will display one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window.
- 5 Click **OK** to continue. When the import is done, a Summary Report is displayed describing the packages that were imported.

- 6 By unchecking the box next to each package, you can choose to import a package without installing it. The default is to install all imported packages.



Packages, like other resources, are always displayed under the user folder in which they were created. Upon import, the Summary Report shows the URI or full path into which the package was imported (for example, "Packages Imported: /All Packages/Personal/Vicky's Packages/VPN Logins Reporting"). The import location is not configurable. If you log in with a different username and import a package, you may or may not have write access to the package (depending on permissions). If you import the package with a different username on a Manager that does not include an account for the package originator, you will not see the imported package. If you recreate an account on the Manager with the same username as the package originator, the imported package will be visible again.

For more information, see ["Resolving Package Conflicts" on page 135](#).


## Exporting Packages

- 1 Click the **Packages** tab in the Navigator panel and click to select one or more packages to export.
- 2 Right-click and choose **Export Package to Bundle**.
- 3 Enter a name and folder for the local bundle file. The default extension is **.arb**.

The exported bundle will have reference IDs if that box was checked in the Package Editor, and it will be obfuscated if that box was checked in the editor.

## Installing Packages

If you chose not to install a package when its bundle was imported, or if you left the Installed checkbox unchecked when you created a package, it will be uninstalled. Uninstalled packages are not shown in the Normal view of the package tree.

- 1 Click the **Packages** tab in the Navigator panel. If the  icon is not highlighted, click it to switch to the Advanced view.
- 2 Right-click the uninstalled package (shown with a gray icon) that you would like to install and choose **Install Package**.
- 3 Review the dialog for any conflicts. Each conflict will display one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window.

For more information, see ["Resolving Package Conflicts" on page 135](#).

## Uninstalling Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be uninstalled. Choose **Uninstall Package**. (This command is disabled if the package is already uninstalled or if it is locked.)

Uninstalling a package removes its resources from the system and hides the package in Normal view, but it remains in the system and can easily be installed again.

Dependent resources will be deleted automatically unless they are contained in another package.

For more information, see [“Resolving Package Conflicts” on page 135](#).

## Editing Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Change the package name or other properties on the Attributes tab. For more information on package fields, see [“Creating Packages” on page 130](#).
- 4 Click the **Resources** tab to add or remove resources from the package.

## Adding Resources to Packages

You can add to a resource to an existing package by using the right-click menu on a selected resource in the Navigator tree.

- 1 Click the **Resources** tab in the Navigator panel.
- 2 Choose the resource type you want to add (for example, Reports).
- 3 Navigate to and right-click the particular resource you want to add (for example, My Report), and choose **Add to Package**. The system displays the Package Selector dialog.
- 4 Select a package to which to add the selected resource and click **OK**.

## Removing Resources from Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Click the **Resources** tab in the Package Editor.
- 4 In the upper half of the Resources tab, select the resource you want to remove. (A gray highlight on the entire row indicates the resource is selected.)
- 5 Click **Remove**.

## Deleting Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be deleted and choose **Delete Package**.
- 3 Confirm that you want to delete the specified package.
- 4 Choose **Remove Resources in Package** or **Leave Resources**. If you Leave Resources, only the package itself will be deleted. The resource that it contained will remain in the system resource tree. If you Remove Resources, all resources that the package contained will be deleted from the system resource tree.



Deleting a package that contains resources that maintain state--active lists with values, session lists, or trends--will delete the state information as well.

---

For more information, see [“Resolving Package Conflicts” on page 135](#).

## Resolving Package Conflicts

Package conflicts can occur during install, uninstall, delete, or import of packages. Most package conflicts are resolved internally by the ArcSight Manager without the need for user intervention. However, some package conflicts will prompt the administrator for an appropriate course of action from among several options. This section describes two of these scenarios as examples.

If the ArcSight Manager detects package conflicts for a pending package **uninstall**, the Console provides choices for resolving the conflict and proceeding, or aborting the uninstall operation. The options provided depend on the type of conflict detected.

For example, if you attempt to uninstall a package that changed since it was installed, the conflict is indicated and you are asked to choose from the following **Resolution Options**.

Option	Description
Create a new archive for package	Creates a new archive for the modified package (and retains original).
Create new archive for remaining changed packages	Creates new archives for all changed packages before uninstall (retains all originals).
Continue without saving changes	Uninstalls this package without saving changes.
Uninstalls this and remaining packages without saving changes	Uninstalls all selected packages without saving changes.
Abort	Abandons the uninstall process and keeps the package(s) as is.

If the ArcSight Manager detects package conflicts for a pending package import or install, the Console provides choices for resolving the conflict and proceeding, or aborting the import operation. The options provided depend on the type of conflict detected.

For example if you attempt to import a package with content that is older than the currently imported package, the conflict is indicated and you are asked to choose from the following Resolution Options:

Option	Description
Leave newer packages	Leaves the newer packages installed.
Never override newer packages	Completes the import but imports only packages that are newer than those currently installed.
Update packages	Imports the selected packages, and prompts for package conflict resolutions on a per-package basis.
Always update packages	Imports the selected packages, and overwrites newer packages if they exist.
Abort	Abandons the uninstall process and keeps the package(s) as is.

## Managing SmartConnectors

ArcSight SmartConnectors can be configured to optimize their performance and increase their functionality. You can configure SmartConnectors to enable aggregation, batching, and time filter correction functionality. You can also send control commands, from the ArcSight Console, to SmartConnectors to manage the flow of events.

### Selecting and Setting SmartConnector Parameters

From the Console, use the Connector Editor to control SmartConnectors.

#### Configuring the SmartConnector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to manage and choose **Configure**. This opens the **Inspect/Edit** panel for the **Connector Editor**. On the Connector tab, the Name field is automatically populated with the name assigned during SmartConnector Installation.
- 3 Type in the **Connector Location** and the **Device Location**. All events are tagged with these fields by the ArcSight SmartConnector. Creation date and other information is automatically populated.
- 4 On the Default tab, change any additional Batching, Time Correction or other parameters as desired, using the configuration fields explanations provided below.
- 5 Click **Apply** to add your changes and to keep the Connector Editor open. To apply your changes and close the Connector Editor click **OK**, or, if applicable, click **Add Alternate** to save your changes as an alternate configuration you can select and apply later.

The description entry associated with the setting provides tool tip information. These parameters are not localized since they come directly from the connector and the connector may contain new resources (since it may be a newer version).

The framework for connector commands operates in a similar way. Configuration of the connector command menu is achieved by sending the list of commands that are supported on the connector at registration time.



The ArcSight Console doesn't currently provide support for command parameters.

There are several controls you can adjust in the Connector Editor. The variety of options are best summarized by briefly describing what's available at each of the editor's tabs or subtabs.

#### Connector Editor Option Tabs

**Table 4-6** Connector Editor Option Tabs

Connector Tabs	Options
<a href="#">Connector Tab Configuration Fields</a>	Basic identification, ownership, and date/time parameters.



Connector Tabs	Options
Networks	The ArcSight network(s) to which the connector is or can be assigned.
<a href="#">Default Content Tab Configuration Fields</a>	Includes options for report batching, aggregation, and time corrections.
Default: Filters	A filter condition editor for constraining what the connector reports. (Please see <a href="#">“Managing SmartConnector Filter Conditions”</a> on page 152 for details on how to define filters for connectors.)
Alternate: Content	A set of options identical to those under Default, which you can use to create alternate configurations.
Alternate: Filters	A filter condition editor for constraining what the connector reports, in an alternate configuration.
Notes: Table	A text editor for, and tabular list of, configuration notes.
Notes: List	A text editor for, and text presentation of, configuration notes.

## Connector Tab Configuration Fields

You do basic configuration through the Connector and Default: Content tabs. Many of these fields correspond to resource editor fields. See also [“Common Resource Attribute Fields”](#) on page 189.

**Table 4-7** Connector Tab Configuration Fields

Name Field	Value Field
Name	The Name text field is automatically populated with the name assigned during SmartConnector installation.
ID	The identification string assigned during SmartConnector installation.
Status	The SmartConnector's current mode of operation.
Connector Location	A description of the (usually) physical location of the SmartConnector. This appears in all the events issued from the connector.
Device Location	A description of the (usually) physical location of the device the SmartConnector is monitoring. This appears in all the events issued from the connector.
Version	The connector's software version number.

Name Field	Value Field
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight ESM. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your ArcSight ESM administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight ESM. A given alias will appear in place of the resource's name everywhere it may be seen. Your ESM administrator can advise you on the correct values for this field, if applicable.
Description	A text description of the configuration or other related information. This text appears as a tooltip to any ArcSight user who has Console access to the connector.
Owner	An ArcSight ESM user selected from the Users resource tree who should be notified about this connector.
Notification Groups	The ArcSight ESM user groups selected from the Users resource tree who should be notified about this connector.
Created By	A user identity provided at SmartConnector installation.
Creation Time	The time of SmartConnector installation.
Time Since Creation	A value calculated from Creation Time.
Last Updated By	The time of the last configuration change.
Last Update Time	The time of the last configuration change.
Time Since Last Update	A value calculated from Last Update Time.

## Default Content Tab Configuration Fields



SmartConnector configuration options available may vary depending on which version of SmartConnectors you are using. SmartConnector configuration options come directly from the connector, and newer versions of connectors might contain new or different resources than previous versions.

**Table 4-8** Default Content Tab Configuration Fields

Name Field	Value Field
<b>Batching</b>	SmartConnectors can batch events to increase performance and optimize network bandwidth. When activated, SmartConnectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires. You can also prioritize batches by severity, forcing the SmartConnector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, 100 events).
Enable Batching (in seconds)	The SmartConnector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is <b>Time Based</b> if the SmartConnector should send batches as they arrive (the default) or <b>Severity Based</b> if the SmartConnector should send batches based on severity (batches of Highest Severity events sent first).
<b>Time Correction</b>	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the SmartConnector to automatically correct the time reported by the device.
Use Connector Time as Device Time	( <b>No</b>   Yes) Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. The default is <b>No</b> .
Enable Device Time Correction (in seconds)	The SmartConnector can adjust the time reported by the device <a href="#">Detect Time</a> , using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol.
Enable Connector Time Correction (in seconds)	The SmartConnector can also adjust the time reported by the Connector Time SmartConnector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the SmartConnector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and SmartConnectors is the NTP protocol.

Name Field	Value Field
Set Device Time Zone To	( <b>Disabled</b>   <TimeZone>)(Default is <b>Disabled</b> ) Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the SmartConnector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported.
<b>Device Time Auto-correction</b>	
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by <b>Past Threshold</b> seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by <b>Past Threshold</b> seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, (ALL) means all devices.
<b>Time Checking</b>	
Future Threshold	These are the time span and frequency factors for doing device-time auto-correction.
Past Threshold	The number of seconds by which to extend the connector's forward threshold for time checking.
Frequency	The number of seconds by which to extend the connector's rear threshold for time checking. Default is 1 hour (3,600 seconds).
<b>Cache</b>	
Cache Size	The SmartConnector checks its future and past thresholds at intervals specified by this number of seconds. Default is 1 minute (60 seconds).
Notification Threshold	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Notification Frequency	SmartConnectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the SmartConnector receives bursts of events. This parameter specifies the disk space to use. The default is <b>1 GB</b> which, depending on the connector, can hold about 15 million events, but it also can go down to <b>5 MB</b> . When this disk space is full, the SmartConnector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
	The size of the cache's contents at which to trigger a notification. Default is 10,000.
	How often to send notifications once the Notification Threshold is reached. (1 min, 5 min, 10 min, 30 min, 60 min.)

Name Field	Value Field
Payload Cache	If the represented SmartConnector supports it, setting this to <b>True</b> causes the connector to automatically create and populate a cache for device payload data. This capability improves upon the previous ability to manually retrieve individual payloads. The payload data is retrieved from the original device or retained from the received event data, depending on how it operates. The default setting is <b>False</b> . Consult the a SmartConnector's Configuration Guide to find out whether it supports this capability. Changes to this setting take effect after you restart the SmartConnector.
Payload Cache Size	If <b>Payload Cache</b> is <b>True</b> , these choices determine the maximum size of the cache. The cache operates on a last-in-first-out (LIFO) basis.
<b>Network</b>	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the ArcSight Manager. The default is <b>10 seconds</b> , but it can go from <b>5 seconds</b> to <b>10 minutes</b> . Note that the heartbeat is also used to communicate with the SmartConnector; therefore, if its frequency is set to <b>10 minutes</b> , then it could take as much as 10 minutes to send any configuration information or commands back to the SmartConnector.
Enable Name Resolution	( <b>Enabled</b>   Disabled) The SmartConnector tries to resolve IP addresses to host names, and host names to IP addresses, if the event rate allows it and if required. This setting controls this functionality. The Source, Target and Device IP addresses and Hostnames may also be affected by this setting. (Default is <b>Enabled</b> )
Name Resolution Host Name Only	( <b>Yes</b>   No) If set to Yes, for reverse resolution (IP Address to Host name), only the host name field is set. If set to No, the host name is split up and put into both the DNS domain and the host name fields. This affects the source, destination, device and SmartConnector name fields. (Default is <b>Yes</b> )
Name Resolution Domain from Email	( <b>Yes</b>   No) If set to Yes, the host name and DNS domain fields are empty, and the corresponding user name field appears as an email address, then the domain from the email address is put in the DNS domain field. This only affects the source and destination fields. (Default is <b>Yes</b> )
Clear Host Names Same as IP Address	( <b>Yes</b>   No) If set to Yes and the host name field is set to an IP Address that matches the corresponding IP Address field, then the host name field is cleared. This affects the source, destination, and device fields. (Default is <b>Yes</b> )

Name Field	Value Field
Don't Resolve Host Names Matching	<p>By default, host names are resolved to their IP addresses. You have the option to specify a regular expression for all or part of a host name <i>for which you do not want the system to attempt host name resolution to an IP address</i>.</p> <p>When this option is configured, the system will not attempt to resolve host names matching this expression.</p>
Don't Reverse-Resolve IP Ranges	<p>By default, IP addresses are resolved to their domain names. You have the option to specify IP address ranges <i>for which you do not want the system to attempt reverse-resolution to domain names</i>.</p> <p>When this option is configured, the system will not attempt to reverse-resolve IP addresses that fall within any of the specified ranges.</p>
Limit Bandwidth To	<p>A list of bandwidth options you can use to constrain the connector's output over the network. (<b>Disabled</b>, 1 kbit/sec to 10 Mbits/sec.)</p>
Transport Mode	<p>You can configure the SmartConnector to cache to disk all the processed events it receives. This is equivalent to pausing the SmartConnector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (<b>Normal</b>   Cache   Cache (but send Very High severity events)).</p>
Address-based Zone Population Defaults Enabled	<p>This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 because the system has integral zone mapping.</p>
Address-based Zone Population	<p>This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 because the system has integral zone mapping.</p>
Customer URI	<p>Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.</p>
Source Zone URI	<p>When populated, this field shows the URI of the zone associated with the SmartConnector's source address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.</p>

Name Field	Value Field
Source Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated source address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Destination Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's destination address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Destination Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated destination address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Connector Zone UR	When populated, this field shows the URI of the zone associated with the SmartConnector's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Connector Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Device Zone URI	When populated, this field shows the URI of the zone associated with the device's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Device Translated Zone URI	When populated, this field shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.

Name Field	Value Field
Field Based Aggregation	<p>This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, the fields of the two events are the same per the fields listed in the description of <a href="#">"Enable Aggregation (in seconds)"</a> on page 147. However, field-based aggregation implements a more flexible aggregation mechanism; two events are aggregated if only the <i>selected</i> fields are the same for both events. (<b>Note:</b> Field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored, unless "Preserve Common Fields" is set to "Yes".)</p> <p>Field-based aggregation offers several advantages over basic aggregation, including:</p> <ul style="list-style-type: none"> <li>• Control over what fields to aggregate on</li> <li>• Start and end time set to the earliest start time and latest end time, respectively (instead of taking the values from the first event in the group, like basic aggregation)</li> <li>• Option to preserve common fields</li> <li>• Option to sum one or more numeric fields</li> </ul> <p>SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate "accepts" and "rejects" in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.</p> <p><b>Note:</b> The legacy, basic aggregation feature is described in the field description for <a href="#">Enable Aggregation (in seconds)</a>.</p>
Time Interval	<p>Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (<b>Disabled</b>, 1 sec, 5 sec, and so on, up to 1 hour.)</p>
Event Threshold	<p>Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (<b>Disabled</b>, 10 events, 50 events, and so on, up to 10,000 events.)</p>



Name Field	Value Field
Field Names	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. Use <b>Ctrl+click</b> to select multiple fields. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-host names. You can use any of the event fields displayed in the event inspector; the name can contain no spaces and the first letter should not be capitalized.
Fields to Sum	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.  If specified, this set of numeric fields is summed rather than aggregated, preserved, or discarded. The most common fields to sum are <a href="#">bytesIn</a> and <a href="#">bytesOut</a> . Note that if any of the fields listed here are also in the list of field names to aggregate, they are aggregated and not summed.
Preserve Common Fields	(Yes   <b>No</b> ) Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing <b>No</b> , the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events).  SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. ( <b>Disabled</b> , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. ( <b>Disabled</b> , 10 events, 50 events, and so on, up to 10,000 events.)
Fields to Sum	(Optional) Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.

Name Field	Value Field
<b>Processing</b>	
Preserve Raw Event	<p>(Yes   <b>No</b>) Some devices contain a raw event that can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field in the event inspector. This feature is disabled, by default, since using raw data increases the event size and therefore requires more database storage space.</p> <p>You can enable this by changing the <b>Preserve Raw Event</b> setting. If you choose <b>Yes</b>, the serialized representation of the "Raw Event" is sent to the ArcSight Manager and preserved in the <a href="#">Raw Event</a> field.</p>
Turbo Mode	<p>If your configuration, reporting, and analytic usage permits, you can greatly accelerate the transfer of a sensor's event information through SmartConnectors by choosing one of two "turbo" (narrower data bandwidth) modes. The default transfer mode is called <b>Complete</b>, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).</p> <p><b>Complete</b> mode does indeed use all the database performance advances of ArcSight v3.x.</p> <p>The first level of Turbo acceleration is called <b>Faster</b> and drops just additional data, while retaining all other information. The <b>Fastest</b> mode eliminates all but a core set of event attributes, in order to achieve the best throughput. Consider the possible effects such a restricted data set might have from a given device (e.g., on reports, rules, threat resolution) before selecting it.</p> <p>The specific event attributes that apply to these modes in your enterprise are defined in the self-documented <a href="#">\$ARCSIGHT_HOME/config/connector/agent.properties</a> file for the ArcSight Manager. Because these properties may have been adjusted for your needs, you should refer to this file for definitive lists.</p> <p>Only scanner SmartConnectors must run in <b>Complete</b> mode, to capture the additional data.</p> <p><b>Note:</b> SmartConnector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to <b>Faster</b> will not pass all the data possible for a SmartConnector that is set for the default of <b>Complete</b>.</p>

Name Field	Value Field
Enable Aggregation (in seconds)	<p><b>Note:</b> If you have already used this feature for setting up previous SmartConnectors, you can continue to do so. However, ArcSight recommends that you use the new <a href="#">Field Based Aggregation</a> feature as a more flexible option. (Please see <a href="#">"Field Based Aggregation" on page 144.</a>)</p> <p>Here is the description of the legacy "Enable Aggregation" feature, for those of you who are still using it:</p> <p>When enabled, <b>Enable Aggregation (in seconds)</b> aggregates two or more events on the basis of the selected time value. (<b>Disabled</b>, 1, 2, 3, 4, 5, 10, 30, 60)</p> <p>The aggregation is performed on one or more matches for a fixed subset of fields:</p> <ul style="list-style-type: none"> <li>• Agent ID</li> <li>• Name</li> <li>• Device event category</li> <li>• Agent severity</li> <li>• Destination address</li> <li>• Destination user ID</li> <li>• Destination port</li> <li>• Request URL</li> <li>• Source address</li> <li>• Source user ID</li> <li>• Source port</li> <li>• Destination process name</li> <li>• Transport protocol</li> <li>• Application protocol</li> <li>• Device inbound interface</li> <li>• Device outbound interface</li> <li>• Additional data (if any)</li> <li>• Base event IDs (if any)</li> </ul> <p>The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.</p>
Limit Event Processing Rate	<p>You can moderate the SmartConnector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts.</p> <p>The choices range from <b>Disabled</b> (no limitation on CPU demand) to <b>1 eps</b> (pass just one event per second, making the smallest demand on the CPU).</p> <p>Be sure to note that this option's effect varies with the category of SmartConnector in use, as described in the SmartConnector Processing Categories table below.</p>

Name Field	Value Field
Fields to Obfuscate	Using MD5 hashing, this option allows you to specify a list of fields for obfuscation in a security event.
Store Original Time In	This parameter allows you to move the original device receipt time to a specified field if altered by the time correction.
Enable Port-Service Mapping	<p>(<b>Disabled</b>   Enabled)</p> <p>If <b>Enabled</b> and one of the two fields destination port and application protocol is set, and the other is not, the one that is set is used to set the other. For example, if the destination port is 22 and application protocol is not set, then the application protocol is set to ssh.</p> <p>Default is <b>Disabled</b>.</p>
Enable User Name Splitting	<p>(Yes   <b>No</b>) If this is set to yes and the destination user name contains commas in the event, this parameter duplicates that event. Each user name in the list is placed in one of the events.</p> <p>For example, if the destination user name in an event is "User 123, User 456", then that event is sent twice, with the destination user name set to "User 123" in the first and "User 456" in the second.</p> <p>Default is <b>No</b></p>
Split File Name into Path Name	<p>(Yes   <b>No</b>) If this is set to yes and an event's file name field is set but its file path field is not, this parameter splits the file name into a path and a name, placing each part into appropriate fields.</p> <p>For example, if the file name field is set to <code>C:\dir\file.ext</code> and the file path is not set, then the file path is set to <code>C:\dir</code> and the file name to <code>file.ext</code>. The separator character can be either <code>\</code> or <code>/</code> as the system looks to the SmartConnector to determine its platform.</p> <p>Default is <b>No</b></p>
Event Integrity Algorithm	<p>(<b>Disabled</b>   SHA-256   SHA-1   MD5   SHA-512)</p> <p>If this is set to one of the algorithms (such as SHA-256), and the <b>Preserve Raw Event</b> parameter is <b>Enabled</b>, then additional event integrity internal events are generated, normally at a rate of about 1 per 50 normal events.</p> <p>The crypto signature field is <i>also</i> set in each event in the format: "<code>#seq(alg):digest</code>", where <code>seq</code> is a persistent event sequence number, <code>alg</code> is the message digest algorithm, and <code>digest</code> is the hexadecimal message digest.</p> <p>These extra events and the crypto signature field values can be used to verify that no events were tampered with after generation.</p> <p>Supported algorithms are: SHA-256, SHA-1, MD5, and SHA-512.</p> <p>Default is <b>Disabled</b> (i.e., no algorithm is applied)</p>

Name Field	Value Field
Generate Unparsed Events	<p>(Yes   <b>No</b>) If set to yes and some incoming event data cannot be parsed (perhaps because a device has been upgraded since the SmartConnector parser was written), then a special event named "Unparsed Event" is generated. The raw event appears in the event message field.</p> <p>If set to <b>No</b>, the SmartConnector log files indicate the unparsed events.</p> <p>Default is <b>No</b></p>
Preserve System Health Events	<p>(Yes   <b>No</b>) If set to yes, internal system health events are preserved.</p> <p>SmartConnectors generate system health events that provide information about the systems on which they are installed (e.g., disk usage, network memory, JVM memory, percentage of processing of CPU memory usage, and so forth). By default, these events are not retained or passed on to ArcSight destinations like ESM and, therefore, not available for viewing. Setting this option to yes makes them available in the Console.</p>

Name Field	Value Field
Enable Device Status Monitoring (in milliseconds)	<p data-bbox="781 258 1230 285">(&lt;NumberOfMilliseconds&gt;   -1 (disabled))</p> <p data-bbox="781 296 1328 426">If set to a &lt;NumberOfMilliseconds&gt;, the selected SmartConnector generates internal events periodically 1 minute (60000 milliseconds) or greater with the status of the devices for which the connector is receiving normal events.</p> <p data-bbox="781 436 1328 516">These events have the name "Connector Device Status," and are intended primarily for the use of content in ESM v.4.0 SP3 and newer versions.</p> <p data-bbox="781 527 1328 606">Enabling periodic device status monitoring events helps monitor both the SmartConnector and device uptime.</p> <p data-bbox="781 617 1328 672">Device status monitoring events include this information, if available:</p> <ul data-bbox="781 682 1328 972" style="list-style-type: none"> <li data-bbox="781 682 1230 709">• Event name (Connector Device Status)</li> <li data-bbox="781 720 1159 747">• Vendor and Product information</li> <li data-bbox="781 758 1159 785">• Source Address and Host Name</li> <li data-bbox="781 795 873 823">• Zone</li> <li data-bbox="781 833 1024 861">• Last event received</li> <li data-bbox="781 871 1328 926">• Total number of events for the device since the connector started</li> <li data-bbox="781 936 1094 963">• Event count since last call</li> </ul> <p data-bbox="781 974 1328 1087">Device status monitoring events can be set to generate every 1 minute (60000 milliseconds), or less frequently (i.e., a greater number of milliseconds than the minimum).</p> <p data-bbox="781 1098 1328 1211">If you specify a number less than 60000, you will get a warning message in the log indicating that the minimum is 60000 milliseconds (1 minute) and that the system will use the minimum.</p> <p data-bbox="781 1222 1328 1335">If you enter a non-number in the field, this generates an error in the log indicating the value could not be parsed. In this case, the feature will be disabled (and the log message will say that).</p> <p data-bbox="781 1346 1328 1438">In such cases, there is no indication on the Console that anything went wrong because there is no mechanism for the Connector to convey that error.</p>

Name Field	Value Field
Payload Sampling	Payload sampling is used by some SmartConnectors to send a portion of packet payload (as opposed to the complete packet payload) along with the original event. This portion is retrieved using the on-demand payload retrieval in the event inspector.
Maximum Length	<p>This feature allows you to configure the maximum length of the payload sample using the following values:</p> <ul style="list-style-type: none"> <li>• Discard</li> <li>• 128 bytes</li> <li>• 256 bytes</li> <li>• 512 bytes</li> <li>• 1 Kbyte</li> </ul> <p>When the Discard option is chosen, no payload sample is sent inside the original event.</p>
Mask Non-printable Characters	This feature allows you to mask the non-printable characters in the payload sample.

## SmartConnector Processing Categories

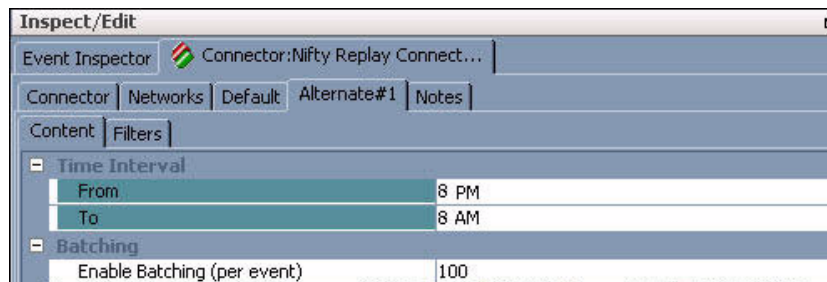
**Table 4-9 SmartConnector Processing Categories**

SmartConnector Type	Effects of Limited Usage
Syslog connectors	Due to the nature of UDP (the transport protocol used by Syslog), these connectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache may fill and the operating system drop UDP messages. Note that ArcSight <b>does not recommend</b> using the <b>Limit CPU Usage</b> option with these connectors because of this possibility of event loss.
SNMP connectors	Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they potentially lose events. SNMP is also UDP-based and has the same issues as Syslog.
Database connectors	Since connectors "follow" the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. On the other hand, note that no events will be lost, unless the database tables are truncated. After the event burst is over, the connector may eventually catch up with the database if the event rate does not exceed the configured limit.

SmartConnector Type	Effects of Limited Usage
File connectors	Similar to database connectors, file-based connectors "follow" files, so limiting their event rates also causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. Similarly, the connectors may catch up if the event rate does not exceed the configured rate.
Proprietary API connectors	These connectors' behavior depends on the particular API, (e.g., OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. Therefore, these connectors work much like database or file connectors.

## SmartConnector Time Interval Options

This time interval applies to the Alternate Settings and it specifies when the alternate settings must be used by the SmartConnector. For example, if you want to cache the events during the day and send everything at night, you can configure the Transport Mode to cache in the default configuration and configure the Transport Mode to normal in the Alternate Settings, then you would set the time interval from 8PM to 8AM (next day).



- **"From:"** Specifies the starting time to apply the Alternate settings.
- **"To:"** Specifies the ending time that the Alternate settings will no longer apply (and revert to the default settings). If this is less than the From setting, the value will be interpreted as "next day". For example, a setting from 8PM to 8AM will be interpreted as starting at 8PM and ending at 8AM the following day.

To save configuration changes to the SmartConnector, click **OK**.

## Managing SmartConnector Filter Conditions

SmartConnector can function as a filtering tool between devices and the ArcSight Manager, using filtering conditions. Filtering conditions are set with a combination of AND or OR statements and data field values. Extraneous events are filtered out to minimize the number of events sent to the ArcSight Manager and analyzed in the ArcSight Console.

### Creating SmartConnector Filters

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the Default | Filter tab, right-click and choose **Add new condition**.



- 4 In the Filter Condition dialog box, select a data field from the drop-down menu. (See “Using Field Sets” under the topic “Common Conditions Editor” in the ESM User’s Guide or Console Help.)
- 5 Choose logic operators from the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

## Adding SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the **Default: Filters** tab, right-click the **if** folder and choose **Add OR** condition to create an OR condition, or right-click the existing filter condition and choose **Add AND condition** to create an AND condition.
- 4 In the Filter Condition dialog box, choose a data field on the drop-down menu.
- 5 Choose logic operators on the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

## Deleting SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector and choose **Configure**.
- 3 In the Filtering section on the Advanced tab, right-click a condition and choose **Delete condition**.

## Setting Special Severity Levels

You can customize or conditionalize the event-severity levels reported by SmartConnectors. Customizing means pre-setting a given SmartConnector’s filter to one specific severity level; conditionalizing is essentially the same, but with the addition of a filter condition to determine when the pre-set severity level is reported.

### Setting a Custom Severity Level

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the appropriate SmartConnector and choose **Configure**.
- 3 In the Connector Configuration Editor, select the Connector: **Default: Filters** tab.
- 4 In the Filters tab, right-click the **Right-click to add an action** item and choose **Add severity action**. The filter shows SetSeverity Very-High.
- 5 Right-click the SetSeverity value and choose a different severity level from the **Set severity** to menu, if necessary.
- 6 Click **Apply** or **OK**.

## Configuring a Conditional Severity

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the appropriate SmartConnector and choose **Configure**.
- 3 In the Connector Configuration Editor, select the **Connector: Default: Filters** tab.
- 4 In the Filters tab, right-click the **Right-click to add an action** item and choose **Add severity action**. The filter shows SetSeverity Very-High.
- 5 Right-click the **SetSeverity value** and choose a different severity level from the **Set severity** to menu, if necessary.
- 6 Right-click the SetSeverity value and choose **Add new condition**.
- 7 In the Filter Condition dialog box choose a field, a logical operator, and enter a value for the condition.
- 8 Click **OK** in the Filter Condition dialog box and **Apply** or **OK** in the Connector Configuration Editor.

For more information, see [“Managing SmartConnector Filter Conditions” on page 152](#).

## Sending Model Mappings to SmartConnectors

Updates to network model mappings are sent automatically from the ArcSight Manager to SmartConnectors within heartbeat messages. The heartbeat messages themselves are sent on an interval which can be anywhere from every 5 seconds to every 10 minutes, but network model mappings are included in the messages only when there are updates to the model.



The interval on which information is exchanged between the Manager and SmartConnectors is determined by the Heartbeat Frequency setting on each Connector. (See information on [“Heartbeat Frequency” on page 141](#) in default content tab configuration fields under [“Selecting and Setting SmartConnector Parameters” on page 136](#).)

---

If you have made several configuration updates to the network model on the Manager and would like these changes to take effect immediately on the SmartConnectors without waiting for the next automatic refresh, you can use the following command to send the update information to a selected Connector.

## Sending Model Mappings to a Connector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to update and choose **Send Model mappings now**.

This sends information about the current network model mappings from the Manager to the selected Connector. It will force a comprehensive refresh of the zone mappings and network model information on the Connector.

## Sending Control Commands to SmartConnectors

From the Console you can issue basic event-flow-control commands to SmartConnectors, get the operational status of a SmartConnector, or issue control commands to network devices through their SmartConnectors. This topic discusses the first two points. To author

rule-driven device-command responses to events, please see “Creating Rule Actions” in the ESM User’s Guide and/or Console Help.

## Getting Status Reports

You can see a SmartConnector’s current operational state at any time.

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command>Status>Get Status**.
- 3 In the Connector Status window you can see a readout of all the connector’s current parameters.

## Sending Flow-Control Commands

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command**, and one of the following menu options described below.
- 3 The Console’s status bar shows a confirmation message when the flow control option takes effect.



- Commands available on this menu will vary depending on which SmartConnectors you are using. The standard set of commands is described here.
- Because there is no local cache, events that occur while a connector is stopped or paused are not retained.
- If a SmartConnector runs out of disk space, it can lose its ability to track events.
- The **Terminate** command should only be used in very special circumstances as it will **kill all** SmartConnector processes.
- See “Creating Rule Actions” in the ESM User’s Guide or Console Help for a description of the rule-based automated alternative for giving SmartConnector commands.

Flow Category	Command	Description
Status	Get Status	Provides a full report on the selected SmartConnector’s current operational state.
	Get Device Status	Provides the status of the device that reports to the SmartConnector. (Currently only available for the CiscoIDS/IPS SmartConnector.)

Flow Category	Command	Description
<b>Connector Process</b>	Restart	<p>Restarts a running SmartConnector.</p> <p><b>Caution:</b> Once a connector is terminated, Console commands cannot access it. Therefore, a "restart" works only on a connector that is currently running. Sending a restart command to a running connector will terminate and restart the connector.</p>
	Terminate	<p>Shuts down the SmartConnector and all processes the SmartConnector started.</p> <p><b>Caution:</b> Once a connector is terminated, Console commands (including Connector Process &gt; Restart) cannot access it. The connector must be restarted manually from the machine on which it is installed.</p>
<b>Event Flow</b>	Pause	<p>Stops the SmartConnector from sending events to the ArcSight Manager.</p> <p><b>Note:</b> Events received from the target device will be saved in the connector cache (even though the connector is in <b>Pause</b> state).</p>
	Stop	<p>Stops the SmartConnector from sending events to the ArcSight Manager.</p> <p><b>Caution:</b> A <b>Stop</b> command causes the SmartConnector to drop all events, including events stored in the connector cache.</p>
	Start	<p>Prompts the SmartConnector (previously in <b>Stop</b> or <b>Pause</b> state) to start sending events to the ArcSight Manager.</p>
<b>Network</b>	Flush Name Resolver Cache	<p>Clears cache for Network name resolver.</p>

Flow Category	Command	Description
Upgrade	Upgrade	<p>Launches a Command Parameters dialog for remote upgrade to newer versions of ArcSight SmartConnectors for managed assets.</p> <p>Provide the version number of the connector to which you want to upgrade and a wait time to verify that the upgrade completed successfully. (If the upgrade is not successful, the system performs an automatic rollback to the previous version of the connector.)</p> <p>Click <b>OK</b> to start the upgrade.</p> <p>See <a href="#">“Upgrading SmartConnectors” on page 166</a> for prerequisites for the upgrade process and detailed information on how to upgrade Connectors.</p>
	Rollback Upgrade	<p>Launches a Command Parameters dialog for remote rollback of connector version to a specified previous version. See <a href="#">“Upgrading SmartConnectors” on page 166</a> for complete information.</p>



Tech Support commands are provided for use primarily by ArcSight Customer Support. Brief descriptions of these Tech Support commands are provided for informational purposes, but these commands are not intended for use by ArcSight customers except as instructed by ArcSight Customer Support.

Flow Category	Command	Description
Tech Support	Get support info	Gets logs and other feedback on SmartConnectors.
	Get 'agent.properties'	Shows the list of properties for the selected SmartConnector.
	Get Upgrade Logs	Get upgrade logs on SmartConnectors.
	Get 'agent.wrapper.conf'	Shows the wrapper configuration for the selected SmartConnector.
	Get Configuration XML File	Shows the XML configuration file for the selected SmartConnector.
	Get Thread Dump	Gets one thread dump for the selected SmartConnector.

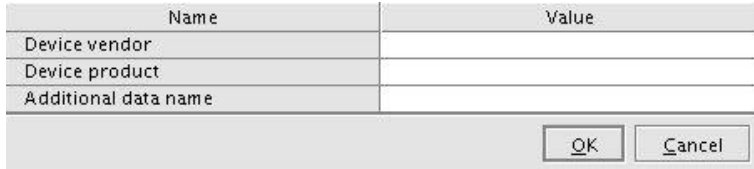
Flow Category	Command	Description
	Get Two Thread Dumps...	Gets two thread dumps for the selected SmartConnector spaced by the time interval specified. By comparing both thread dumps, ArcSight Customer Support can troubleshoot connectors with threads that are hanging for unknown reasons.
	Get last N lines of 'agent.log'...	Shows an excerpt from the connector log file based on the number of lines you specify. The default is 500 lines.
	Get system properties	Shows system properties for the selected connector, including details on variables such as Java runtime name, Java virtual machine (VM) version, operating system name, paths for various Java components, paths for ArcSight Home, user directories, user home, and so forth.
	Enable Event Flow Tracing...	Allows you to specify a component and fields to log for initiating an event flow trace. Component and field names must be provided per appropriate syntax. The component should be chosen from the components listed in the Get Status results.
	Disable Event Flow Tracing...	Disables event flow tracing on the selected component.
	Get Event Flow Tracing Log	When tracing is enabled on the selected connector, the connector logs data about events it receives.



The following commands provide access to SmartConnector component mapping and event categorization for advanced users.

Flow Category	Command	Description
Mapping	Get Additional Data Names	<p>Returns a list of additional data names seen for each device vendor/product combination since the connector started running. For example:</p> <pre>Additional Data Names Seen: Generic (no vendor/product): test1 [3 times] test11 test13 [2 times] Vendor/product [vend/prod]: test1 test10 [6 times]</pre> <p>By default, the command limits the list to show only the most recent 100 device vendor/product combinations and the most recent 100 names for each.</p> <p><b>Tip:</b> You can change this limit by editing the SmartConnector property <code>agent.additionaldata.mapper.track.max.names</code> in the file <code>\$ARCSIGHT_HOME/ArcSightSmartAgents/current/user/agent/agent.properties</code> on the machine where the connector is installed. However, in most cases we recommend keeping the defaults. If you do change a property setting such as this, you will need to restart the connector.</p> <p>If a data name is not a string, its data type is displayed in the list. If the connector saw an additional data name more than once, the command output indicates the number of times the name was seen.</p>
	Map Additional Data Name...	<p>Brings up a dialog where you can map an additional data name for the selected connector.</p>

Name	Value
Device vendor	
Device product	
Additional data name	
ArcSight field	

Flow Category	Command	Description
		<p>For a generic mapping, you can leave the <b>Device vendor</b> and <b>Device product</b> fields blank. For a specific mapping, fill in these fields with the appropriate vendor and product names.</p> <p>Typically, the <b>Additional data name</b> is one of the names shown in the Get Additional Data Names output (but can be another name not on that list).</p> <p>The <b>ArcSight field</b> must be a valid ArcSight event field.</p> <p>Click <b>OK</b> to create the mapping.</p> <p>Here is an example of the command output for a successful generic mapping:</p> <pre>Successfully mapped additional data name [test11] to event field [message] for vendor/product []</pre> <p>A successful device vendor/product-specific mapping returns output similar to this:</p> <pre>Successfully mapped additional data name [test10] to event field [message] for vendor/product [vend/prod]</pre> <p>If the additional data name has not been seen, the name is still mapped, but with a warning like this:</p> <pre>Successfully mapped additional data name [foo] to event field [deviceCustomString1] for vendor/product [vend/prod] (note that additional data name [foo] has not been seen for vendor/product [vend/prod])</pre> <p>If the ArcSight field is not valid, the error returned is similar to this:</p> <pre>Failed to map additional data name [bar] to event field [messages] for vendor/product [vend/prod] (event field [messages] is unknown)</pre>
	Unmap Additional Data Name...	Brings up a dialog where you can unmap an additional data name for the selected connector.
		



Flow Category	Command	Description
		<p>To remove a generic mapping, you can leave the <b>Device vendor</b> and <b>Device product</b> fields blank. To remove a specific mapping, fill in these fields with the appropriate vendor and product names. The additional data name should be one that was previously mapped for the specified device vendor and product combination.</p> <p>Click <b>OK</b> to unmap the data name.</p> <p>Here is an example of the command output for a successful generic unmapping:</p> <pre>Successfully unmapped additional data name [test11] for vendor/product []</pre> <p>A successful device vendor/product-specific unmapping returns output similar to this:</p> <pre>Successfully unmapped additional data name [foo] for vendor/product [vend/prod]</pre> <p>If the specified additional data name was not previously mapped, the output looks like this:</p> <pre>Failed to unmap additional data name [foo] for vendor/product [vend/prod] (not previously mapped)</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• One additional data name can be mapped to more than one ArcSight field for the same device vendor/product combination, and in this case unmapping it unmaps it from all ArcSight fields for that device vendor/product. This is an unlikely scenario, however.</li> <li>• The converse case, where multiple additional data names are mapped to the same ArcSight field for the same device vendor/product combination, results in the last mapping taking precedence over any previous mappings to that ArcSight field for that device vendor/product. No warning is generated in this case.</li> </ul>

Flow Category	Command	Description
Categorizer/ mapper	Reload custom categorizations	<p>There are several ways to set event category information for events. The least common of these is to store custom categorization files (organized by vendor and product) on the connector machine in the <code>user/agent/aup/acp/categorizer/current</code> directory (or the <code>user/agent/acp/categorizer/current</code> directory).</p> <p>If such categorization files exist and have been changed, this command reloads them without restarting the connector.</p>
	Reload custom map files	<p>Rescans and reloads map files in <code>user/agent/map</code> directory on the machine where the connector is installed.</p> <p>The map files are named in the form <code>map.n.properties</code>, where <code>n</code> is a number starting with 0. Changes to these files will be seen periodically in any case, but you can use this command to immediately apply the latest changes. Not all connector setups include custom map files.</p> <p><b>Caution:</b> Map files are created on some connector machines to fulfill specific needs. If you are not familiar with the categorizer/mapping setup of an environment, we recommend that you do not use these commands.</p>



This menu also provides options to test commands.

## Managing SmartConnector Groups

You can best manage ArcSight SmartConnectors when you organize them into groups. You'll find all uncategorized SmartConnectors in the Unassigned group.

You can move or copy groups and SmartConnectors into other groups in the Connectors resource tree by using drag-and-drop. If a group is deleted, the SmartConnectors within that group are also deleted.

You should not delete a Connector resource at the ArcSight Console, unless the corresponding SmartConnector is first stopped. If the SmartConnector on the device is running and its Connector resource is deleted, the SmartConnector will no longer be able to send events to the ArcSight Manager, causing the SmartConnector to start caching events and eventually dropping these events.

## Creating SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **New Group**.  
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

## Renaming SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Rename**.
- 3 In the "name" text field, rename the group.
- 4 Press **Enter**.

## Editing SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Edit Group**.
- 3 In the Group Editor, edit the **Name** and **Description** text field.
- 4 Click **OK**.

## Moving or Copying SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

## Deleting SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

## Managing SmartConnector Resources

This topic describes how to do basic resource management for SmartConnectors.

### Moving or Copying a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.

- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

## Deleting a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

## Importing and Exporting SmartConnector Configurations

As a part of Managing SmartConnectors, you may want to share configurations among several instances of the same or a similar connector.

You can import and export SmartConnector configurations as a means of sharing custom configurations among several connectors on the same or multiple Managers. Rather than redefining a complex configuration on each connector, you can export the configuration as an XML file and then import it into connectors that share some or all of its configuration settings. An override feature allows you to make changes to any of the parameter values upon import.

## Importing a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector into which you want to import a new configuration and choose **Import Connector Configuration...**

This brings up a file browser where you can select the file to import.

- 3 In the file browser, navigate to and select the [.xml](#) file that contains the connector configuration, and click **Open**.



SmartConnector configurations must be saved and imported as XML files.

---

This brings up a dialog showing original and proposed new configuration settings for the selected connector, with an option to override any of the proposed new values. (Click **Show** to show the details of the import or **Hide** to hide them.)

- On the Import Connector Configuration dialog, review the import information and override any values that you do not want to import.

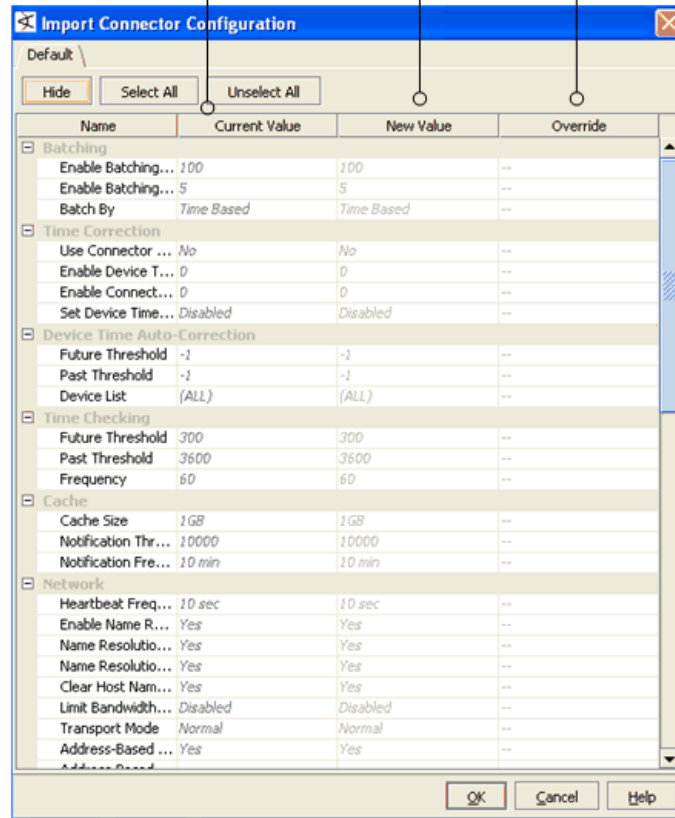
This dialog shows original values for the selected connector configuration and new values that will be applied upon import. You can override any of the settings you do

not want to import by either keeping the parameter value in the original configuration or defining a new value.

For example, you even can limit the import to only filters by keeping all values in the original configuration and choosing to override only the filter values with the imported values as is detailed in SmartConnector Filters. (Scroll down to the Filters section at the end of the Import dialog to see the filters.)

Before import, the Import Connector Configuration dialog shows current value, new value, and override option for each aspect of SmartConnector configuration.

You can accept all new values or override the import by keeping some of the original values.



- When you are satisfied with the settings to import and overrides (if any), click **OK** to import the configuration.

## Exporting a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to export, and choose **Export Connector Configuration As...**

This brings up a file browser where you can navigate to the location where you want to save the configuration as an XML file.

- 3 In the file browser, navigate to and select the location where you want to save the configuration, provide a name for the file, and click **Save**.



SmartConnector configurations must be saved as XML files.

## SmartConnector Filters

You can import and export only the filters associated with SmartConnectors as a part of an import or export on a SmartConnector.

- To export a SmartConnector filter, export the connector that uses the filter (as described in the previous topic on exporting a SmartConnector configuration).
- To import a SmartConnector filter into another connector, start by selecting in the Navigator the SmartConnector to which you want to add a new filter. Follow the steps to import the connector that includes the filter you want to import (as described in the topic on importing a SmartConnector configuration). On the Import Connector Configuration dialog, limit the import to only the filter(s) you want by keeping all values in the original configuration and choosing to override only the filter values with the import. (Scroll down to the Filters section at the end of the Import dialog to see the SmartConnector Filters.) When you have the new, imported filter values selected to override those in the original connector, complete the import by clicking **OK** on the Import Connector Configuration dialog. This adds the imported filter(s) to the original SmartConnector.

## Upgrading SmartConnectors

ArcSight Enterprise Security Management (ESM) now provides the ability to not only centrally manage and configure SmartConnectors, but also to update them remotely. You can use the Upgrade command on the Console to upgrade to newer versions of ArcSight SmartConnector software for managed devices. (And you can use the Rollback command to revert to a previous version on an upgraded connector.)

The Upgrade command lets you launch, manage, and review the status of upgrades for all SmartConnectors. A fail-over mechanism launches SmartConnectors with previous versions if upgrades fail. All communication and upgrade processes between components (Console, Manager, connectors) take place over secure connections.

The ArcSight Console reflects current version information for all of your SmartConnectors.



For this release, SmartConnector remote upgrade is supported for connectors installed on Linux, Solaris, and Windows platforms only.

---

## Overview of the Upgrade Process

- 1 As an ArcSight customer, you will receive an e-mail notification about new connector releases from ArcSight support.
- 2 ArcSight administrators download the latest releases to the ArcSight Manager where they are available for SmartConnector upgrades.

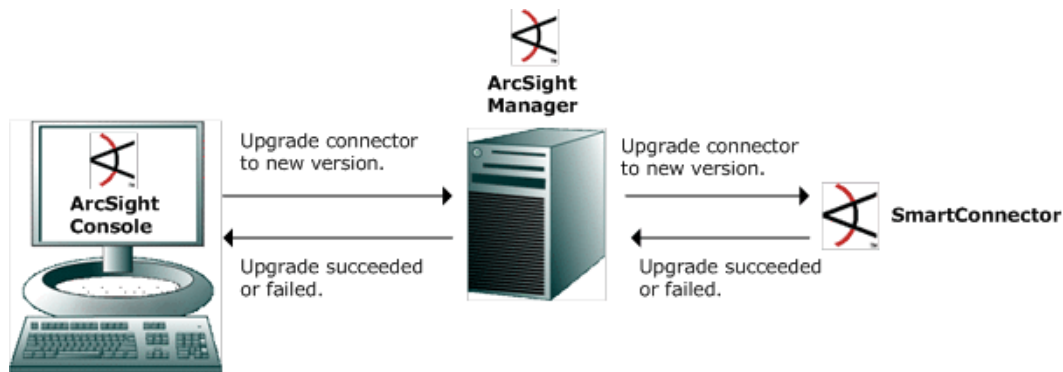


SmartConnector "upgrade" version files are delivered as ArcSight Update packs (**.aup**) files. (ArcSight update packs are compressed file sets, similar to **.zips**.) The administrator copies the **.aup** file to `ARCSIGHT_HOME/updates/` onto a running Arcsight Manager. The Manager automatically unzips the **.aup** file and copies its contents to `ARCSIGHT_HOME/repository/`.

---

- 3 From the ArcSight Console, administrators select connectors to be upgraded (one at a time) and launch the upgrade command for each of them.

- 4 Upon receipt of the upgrade command, the selected connectors upgrade themselves, restart, and send upgrade results (success or failure) back to the ArcSight Console through the ArcSight Manager.
  - ◆ If the upgrade is successful, the new connector starts and reports on successful upgrade status. (The upgraded connector runs in the same home directory as the old connector.)
  - ◆ If the upgraded connector fails to start, the original connector restarts automatically as a fail-over measure. (This is essentially an automatic rollback, and re-start).



#### Tips on Monitoring SmartConnector Upgrade Status

SmartConnectors automatically determine their upgrade status when they start.

- When a connector starts up, it determines whether it is upgraded.
- If so, it waits for a configurable time interval for events from the monitored device to be processed.
- If, after that time interval, events have been processed, the SmartConnector is deemed up and running. The Console indicates that the upgrade for that connector is a success and the newer connector version is reflected.



#### Notes on SmartConnector Upgrade Procedure

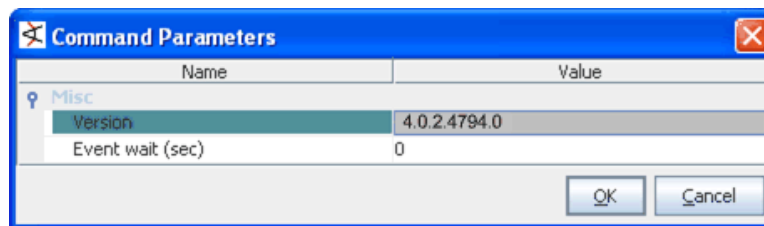
- When upgrading SmartConnectors, be sure to download current versions of the connector Configuration Guides from the ArcSight Customer Support Web site. New or revised information is provided in these guides as appropriate per each release of SmartConnectors. (To check version numbers on your current connectors, see [“Getting Status and Versions on Installed SmartConnectors”](#) on page 169.)
- You need administrative permissions to upgrade connectors.
- Newer versions of the connectors you want must be available on the Manager to which you are connected.
- The option for remote upgrade is available only in ArcSight ESM v.4.0 Console and only on SmartConnectors of version 4.0.2.xxxx.0 or newer. Earlier versions of Connectors (or Agents) must be upgraded manually as per the original process by installing a newer version of the connector.
- As a prerequisite to upgrading connectors, both the ArcSight Manager and the connector you want to upgrade must be running.

The **Upgrade** SmartConnectors command is available as one of several SmartConnector control commands.

## Upgrading SmartConnectors

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Upgrade**.

This launches a Command Parameters dialog.



- 3 Provide the following information in the dialog.
  - **Version** - The Version field provides a drop-down menu showing the connector versions available on this Manager. Choose the Version number of the connector to which you want to upgrade.
  - **Event wait (sec)** - Number of seconds the upgrade process will wait for the first event from the device after the new, upgraded connector is started. If no events are received from the device within the specified time frame, the upgrade is considered "failed" and the old connector is launched.

This optional check is an additional safeguard against upgrade failures. For example, the connector binaries may have been upgraded successfully, but the new version may have problems communicating with the device. In that case, this check will assume that the upgrade failed and bring back the old connector.

If the **Event wait (sec)** value is **0** (the default), then the upgrade does not perform this check.

- 4 Click **OK** to close the dialog and start the upgrade.

As the upgrade proceeds, the connector will show as "down" and then "running" again in the resource tree. Status messages on the Console will indicate whether the upgrade succeeds or fails. You can check the logs for the connector to determine if the upgrade succeeded. (**Send Command > Tech Support > Get 'agent.properties' and Get Upgrade Logs.**)



## Rolling back to a Previous Version



### Notes on SmartConnector Rollback Procedure

- You need administrative permissions to roll back Connectors.
- The option for SmartConnector rollback is available only in ArcSight ESM v.4.0 Console and only on SmartConnectors of version 4.0.2.xxxx.0 or newer that have been previously upgraded.
- Rollback automatically reinstates the most recent version prior to the currently installed version. You cannot do a remote rollback on a connector to other than the previously installed version. (For example, if you start with a connector of version 4.0.2.4793, upgrade to 4.0.2.4794, then upgrade again to 4.0.2.4795, a remote rollback at this point will re-install/start connector version 4.0.2.4794. If you wanted to roll back to an earlier version, you would need to do this manually.)

You can roll back an upgraded connector to the previous version with the Rollback command.

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Rollback**.

As the rollback proceeds, the connector shows as "down" and then "running" again in the resource tree. You can check the logs for the connector to determine if the rollback succeeded. (**Send Command > Tech Support > Get 'agent.properties'** and **Get Upgrade Logs**.)

## Troubleshooting

If an upgrade or rollback fails, you can review the related logs. Choose **Send Command > Tech Support > Get Upgrade Logs** from the ArcSight Console menus.

You can also use the Send Logs wizard to collect and send logs, including upgrade logs, to ArcSight for support help.

### Getting Status and Versions on Installed SmartConnectors

Before or after you upgrade a SmartConnectors, you may want to check version numbers of currently installed connectors or get other status information. There are several ways to get information on currently installed connectors (including various control commands, channels, dashboards). Two of these are highlighted here as easy ways to get connector version information.

#### Getting Status on a SmartConnector

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Status > Get Status**.

The Status information on a connector includes "Agent Version" near the top of the message window. Here is an example snip-it of the Get Status command results for a Test Alert connector, Version 4.0.2.4793.0:

```
Status Generated: Wed Mar 07 13:20:09 PST 2007
Memory Usage: 65Mb out of 253Mb

Agent Content Version.....2007-03-01-09-02-05_4793
Agent Type.....testalertng
```

```

Agent Version.....4.0.2.4793.0
CommandResponses Processed.....1097
Current Max Rate.....22
Event rate LTC.....Wed Mar 07 13:18:42 PST 2007
Events Processed.....24003

```

### SmartConnector Dashboards

Choose **Dashboards** from the Navigator panel, and expand the folders to find various dashboards. To view a dashboard, right-click it and choose **Show Dashboard**.

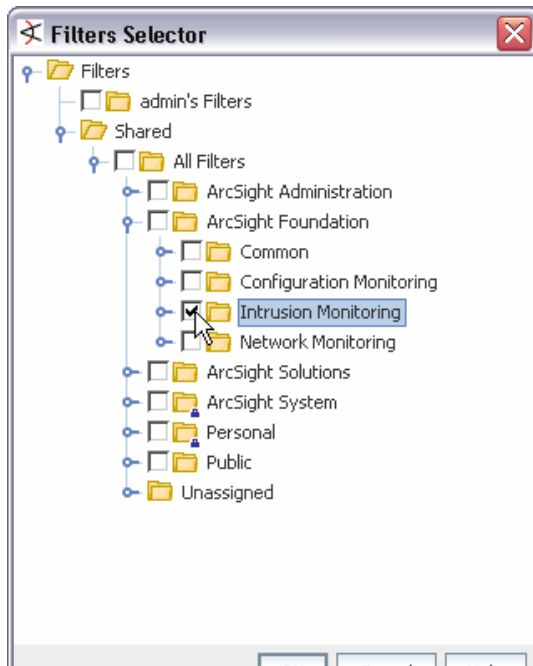
You can find some these SmartConnector dashboards in /Dashboards/Shared/All Dashboards/ArcSight Administration/Connector/:

- Connector and Device - Heads Up Display
- Connector Status

## Selecting Resources

You often need to select resources to act on or use while authoring or configuring analysis tools. Selecting is often the first step in managing, authoring, or analyzing resources.

While the Navigator panel is your usual means of selecting resources, you can also encounter the Select Resources dialog box any time selection is a necessary part of some task, such as adding a case group to a rule action or adding user groups to access control lists (ACLs).



For resource groups, click to highlight and select the group you want to choose, then click **OK**. For options that allow multiple selections, select the check boxes next to individual entries in the list under a group, then click **OK**.

This dialog is also displayed for setting user permissions on resources and operations.

For information about setting permissions on resources, see [“Managing Permissions and Resources” on page 81](#).

For information about setting action permissions on who can deploy data monitors, see also [Step 4 on page 91](#) in “Controlling Who Has Permissions to Deploy Data Monitors” on [page 90](#).



## Finding Resources

Apart from visually navigating the resources in the Navigator panel, you can also find items in busy resource trees by searching or by locating them.

### Searching for System Resources

The search capability uses conventional query elements to search the entire set of system resources, returning a ranked list of qualifying items. Each user sees only those resources for which they have permission, regardless of the query. You can search for a string in All Resources or within a particular resource with both of the following methods.

#### Search Field on Console Tool Bar

In the Search field  on the Console toolbar type a name or phrase and click the Find Resource button (  ). The Search hits are displayed in the Viewer. Single-click an item to display a preview of its definition in the Details pane on the Viewer, or double-click it to open its definition in an Editor in the Inspect/Edit panel.

To limit a search to a particular resource type, click the **drop-down menu** tab on the Search field and choose a resource type from the menus. Notice that some resource types have sub-types from which you can choose. If you limit the Search to a resource type, an icon representing the resource type you are searching on is displayed in the Search field (instead of the standard looking glass Search icon).

For example, to search for a name or phrase only in Trends, choose **Reports > Trends** from the Search drop-down, enter the search string, and click the **Find Resource** button.

The Search field in the toolbar accepts all the Query Options described below.

To limit the Search to items of a particular resources, click the Search drop-down button and select a resource type, then enter the Search string and click the Find Resource button.

Note that some resource types have sub-types you can select; e.g., Reports > Trends.

Type the name or phrase associated with the item you are searching for (you can include spaces in the Search string; e.g., VPN Logins) and click the Find Resource button.

Search results are shown in the Viewer panel on a Find Resource tab.

Single-click a found resource to get a Details preview of it.

Double-click the item to open it in an Editor.

As an alternative to using the quick Search field option, you can get a full Search panel in the Viewer:

- 1 Choose **Edit > Find Resource** in the Console's menus, or press **Ctrl+F**.
- 2 In the Viewer panel's Resource Search tab, enter a query string in the **Search query** line, set the number of results to allow, and click **Find**. See ["Query Options" on page 172](#).
- 3 When the search returns its results, click any item to see its details or click a result column heading to change the order.

When you click a resource listing in the **Details** panel, it shows you the various pieces of related system information that justified that item's ranking.

## Query Options

Pose your queries using these conventions.

Query Elements	Descriptions	Examples
Full or partial strings	Phrases, words, or partial words.	"Attack Notification" notification notif

Query Elements	Descriptions	Examples
Wildcards	Question marks (?) for single-character substitutions and asterisks (*) for multi-character substitutions.	<code>attack??</code> (attacker, attacked) <code>notif*</code> (notify, notifier, notification)
Boolean Operators	Use <b>AND</b> and <b>OR</b> to join strings.	attack <b>AND</b> suspicious <b>AND</b> high
Fields	Resource field labels (grid view columns) followed by a colon, with the data expressed as plain strings, Boolean strings, quoted strings, or parenthetical expressions.	<code>type:datamonitor AND name:"event counts"</code> <code>name:"address space"</code> <code>name:(address+space)</code> <code>name:(+address space)</code>
Exclusion	Use NOT, the minus sign (-), and the exclamation point (!) to exclude strings.	<code>at???? - attack at???? NOT attack at???? AND !attack at???? AND !attack AND !type:zone</code>
Proximity	Extend data-field queries' scope with a proximity factor expressed as a numeral following a tilde (~). The numeral sets the maximum number of words allowed between the specified words in the resources found.	<code>name:("top events"~1)</code> (top attack events) <code>name:("top events"~2)</code> (top serious attack events)
Fuzzy	Broaden query results with a relative letter-substitution factor expressed as a decimal fraction following a tilde (~). The values 0.0 to 0.9 apply, with the higher values increasing the substitutions made in the string.	<code>name:mssp~0.2</code>

## Result Columns

Click any column heading to toggle between descending and ascending order.

Column	Description
Score	Ranking of resources a query returns, based how frequently the search term appears in each resource.
Type	Top-level categorization of the resource, as shown on the Navigator panel.
Name	The full name of the individual resource.
URI	Full uniform resource identifier for the individual resource.

## Locating Specific Resources

The resource trees in the Navigator panel are handy for finding and using the security assets available in your organization and provided by ArcSight. However, when you are working with a particular resource in an editor or grid view, locating that item's position in a heavily populated resource tree can be inconvenient.

You can use two right-click commands to instantly spot resource entries in the Navigator panel, from applicable grid view resource listings or resource editors.

- 1 In an entry in a resources grid view, or in the top tab of a resource editor, right-click and choose **Find <asset type> in Navigator**.
- 2 Look for the highlighted item in the Navigator panel's resource tree.

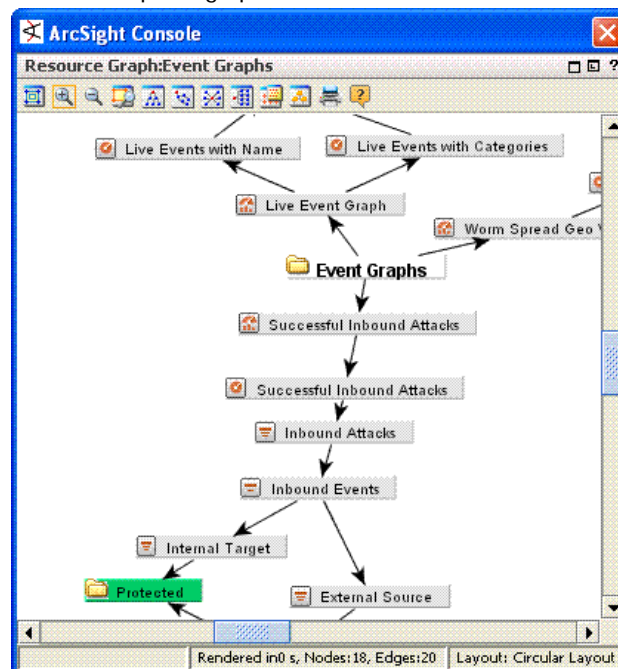
## Visualizing Resources

The resources presented in the Navigator panel or graphically in the Viewer panel are organized into hierarchical groups for easy browsing. Among similar types of resources, there can be logical relationships. Graphs can make these relationships readily visible.

### Graphing Resources

- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.











The Viewer panel graphs the resources in a new channel.





### Using Graphs

Once generated, you can manipulate graphs further. There is a set of command buttons at the top of the view and a parallel set of commands available by right-clicking the graph itself.

**Table 4-10** Resource Graph Buttons and Right-click Commands

Command	Button	Description
Inspect		Opens a new event-monitoring channel, using the visualization's current timeframe, event and node filters.
Refresh		Updates the graph.
Fit Content		Sizes the graphic to the available display space.
Zoom In / Zoom Out		Increases or decreases the size of the displayed graphic.
Zoom Selected		Zooms in on a selected portion of a graphic.
Hierarchic Layout		Presents nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing event relationships that have a common root.
Organic Layout		Displays nodes in an arrangement based on minimum edge length, which tends to cluster nodes that relate to a common node. Likewise, node clusters with nodes in common will also tend to group together.
Circular Layout		Positions nodes in hub-and-spoke arrangements with each node radiating edges to, or receiving edges from, the nodes with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout instead.
Orthogonal Layout		Arranges nodes on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are very useful for clearly tracing connections and identifying node clusters.
Overview		Opens a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.
Hierarchy Tree		Opens a complete list of the nodes plotted in graphic layouts. Click a node in the list to scroll to that node in the main view.
Print		Prints the displayed graphic.
Export to JPEG		Create and save a JPEG-format copy of the current image.

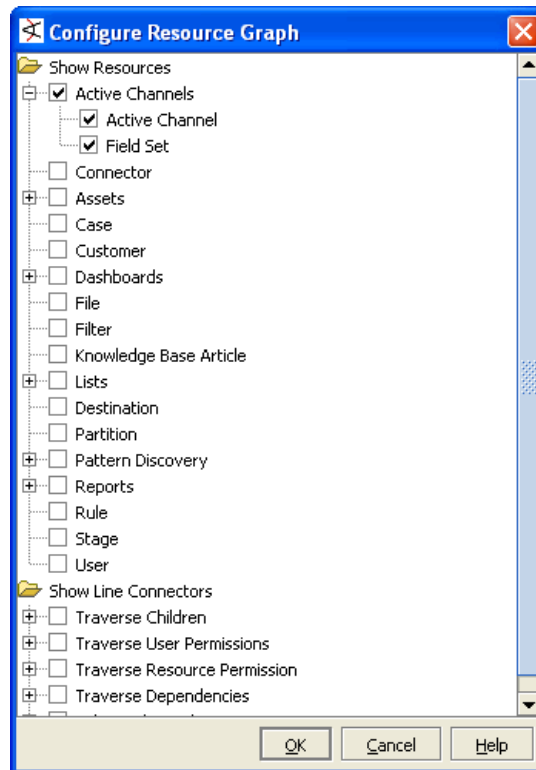
Command	Button	Description
Add Graph View to Case		Adds the current graph view to a case you select. Choosing this option opens the Case Selector dialog, where you can browse cases. Select a case to which to add the current graph view and click <b>OK</b> on the Case Selector dialog. The graph view is added to the selected case as an attachment, accessible on the Attachments tab in the case editor for that case.
Help		Display the relevant ArcSight Console online Help topic.
Snapshot		Creates a new copy of the visualization itself. This graphic is not associated with a dashboard, even when starting from a dashboard viewer.
Snapshot Selection		Opens a new visualization that contains only the selected nodes and their connecting edges.

## Configuring Resource Graphs

- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.
- 4 Hover cursor or click anywhere in the Viewer panel, and right-click **Configure Resource Graph** option on the context menu.



This brings up the Configure Resource Graph dialog where you can specify which resources to display in graph views.



- 5 Select resources to show or hide. (Click checkboxes to toggle show/hide options on resources. Resources with check marks are configured to show for the selected graph view.)
- 6 Click **OK** to save your changes.

For more information, see [“Selecting Resources” on page 170](#).

## Viewing Resources in Grids

While the grids you see in the Viewer panel are most often views of events, these grids can also display organized sets of information about resources in the Navigator panel.

In the Navigator panel, certain resource groups include **Grid View** in their right-click context menus. This command causes the items in the group to display in a grid view, where you can review them using the sorting and column customization features that grid views offer. You can also right-click resource items in grid views and use the same context commands that those resources have in the Navigator panel.



## Validating Resources

Resources can break or become invalid because they are improperly built or cannot find other resources they depend on. The following topics describe how to identify valid and invalid resources, show how to troubleshoot and fix broken resources, list requirements for valid resources, and provide tips for manual and automatic resource validation.

## Valid and Invalid Resources

Valid resources show up in the Navigator with their associated icons as described in "Navigating" in the ESM User's Guide or Console Help.

A resource can "break" or become "invalid" either because it is constructed improperly (for example, when an active list schema does not match the underlying table) or because another resource it depends on is missing from the database (for example, when a rule references an unavailable filter). The latter can happen when a resource used in other resources is deleted from the Manager, or not retained during an upgrade, import, or export.

Invalid resources show up in the Navigator as broken or torn. For example, the Navigator displays a valid filter like this: , and an invalid filter like this: . An invalid resource also includes an "Invalid Reason" field under on the Attributes tab of its editor, as described in [Common Resource Attribute Fields](#) under "Invalid Reason" on page 190.



A valid resource is fully available to other resources that reference it, and can participate in the event flow, trends, reports, data monitors, channels, filters, rules, and so forth.

An invalid resource cannot participate in the event flow or other resources in real time. For example, an invalid asset cannot participate in event asset resolution. Correlated events in which the source or target address points to the invalid asset are not generated. Similarly, an invalid rule does not trigger and generate correlation events.

## Fixing and Validating Resources

When a resource become becomes invalid, its Editor includes a **Validate** button that you can use to test and validate the resource after you fix it. Clicking the **Validate** button on a resource that was previously broken results in a check of the resource logic and dependencies. If the system determines the resource is now valid, the resource icon in the Navigator is updated to reflect a working resource. If the system determines the resource is still broken, it displays an error message describing the problem.

The general flow of steps to fix and validate a resource are:

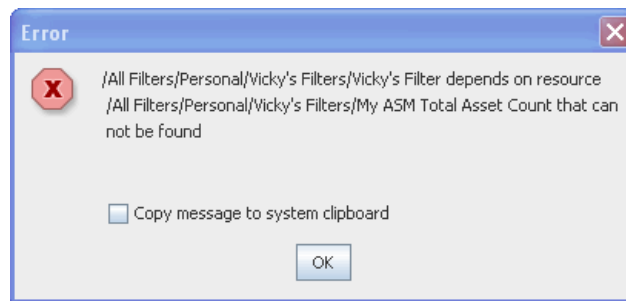
- 1 Identify an invalid resource. Sometimes problems with filters or rules (which are used in many other resources) are a result of broken resources. (A valid resource looks like this: , and an invalid resource looks like this: )

For example, if "My Top Threats" filter depends on "My Hotlist" filter, removing "My Hotlist" filter breaks "MY Top Threats" filter.

A scheduled job (like a scheduled rule group or archived report) can also break if one of the resources it depends on is missing. The broken icon for a scheduled job shows up on the Current Jobs list.

- 2 If you do not already know why a resource is broken, open its editor (double-click the resource in the Navigator panel) and click the **Validate** button in the resource editor.

This will give you an error message that describes the problem. The error dialog includes a Copy button for copying longer messages to an external editor.



- 3 Fix the problems with the resource. This may involve adding back in missing resources or rebuilding the resource to fit various other requirements as described in Troubleshooting Invalid Resources below.

To continue with our example, adding back in the filter "My Hotlist" would fix the problem we mentioned in step 1.

- 4 In the resource editor(s), click **Apply** to save changes to the resources you modified.



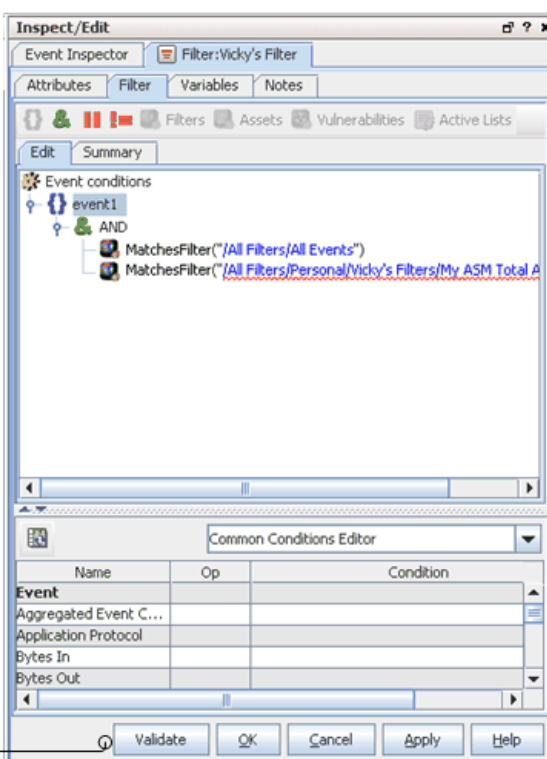
For problems that can be validated on the local client, you can click **Validate** before clicking **Apply** and if the resource is fixed its "working" icon is immediately reflected in the Navigator. However, for other types of problems; you need to **Apply** the changes to the resource before you **Validate** the resource. This is because some types changes must be processed on the Manager to determine dependencies and relationships to other data not available on the local client.

If you think you have fixed a resource but it is still not showing as fixed in the Navigator, make sure you **Apply** all the changes you made to it and then click **Validate** again.

- 5 In the resource editor for the resource that was broken, click **Validate**. If the resource passes validation, its icon in the Navigator updates to reflect a working resource.

In the resource Editor for the resource that was broken, click **Validate** button. If the resource passes validation, its icon in the Navigator updates to reflect a working resource. Otherwise, the broken icon remains and an error message describes the problems.

Some problems require saving fixes to the Manager, so be sure to click **Apply** and save changes to resources you fix before you click **Validate**.



To validate a scheduled job, click the **Open scheduled jobs list** tool button (🕒) to display scheduled jobs in the Viewer, right-click the job you want to validate, and choose **Validate** from the context menu. If the job passes validation, its icon in the Current Jobs list updates to reflect a valid task.

## Troubleshooting (Requirements for Valid Resources)

The most common cause of an invalid resource is a dependency issue; another resource that the broken resource depends on is missing from the database. Some resources have additional requirements or limits that can also affect validity. Following is a summary of requirements for creating valid resources.

If any of these requirements are not met, the resource will break. To fix the resource, edit its definition to be in line with these requirements.

- All Resources - If the definition for a resource references another resource, the referenced resource must be available in the Manager database. This requirement is true for all types of resources.
- Devices and Assets - Each asset address must be unique within a zone, an asset can belong to one zone only, and the asset IP address must fall within the address range of its network zone.

- Device and Asset Ranges - Start addresses must be less than end addresses, asset ranges must be within the address range of the associated network zone, and asset ranges should not overlap another asset range in the same zone.
- Zones - Start addresses must be less than end addresses and network zones should not overlap other zones in the same network.
- Reports - Report templates cannot contain more than 20 charts or more than 15 tables.
- Active Lists - Active List schema must match the underlying table and must not include programming errors.

Resources become invalid when they violate one or more of their constraints. The following table lists the resources that can become invalid:

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Device/Asset	<ul style="list-style-type: none"> <li>Asset address must be unique within a zone</li> <li>An asset only belongs to one zone</li> <li>Asset IP address must fall in the address range of its network zone</li> </ul>	The invalid device/asset can not participate in the event asset resolution. Therefore, if an event has source/target address pointing to the invalid device it will not be resolved.
Device/Asset Range	<ul style="list-style-type: none"> <li>Start address must be less than end address</li> <li>Asset range must be within the address range of its network zone</li> <li>Asset range should not overlap another asset range in the same zone</li> </ul>	The invalid device/asset range can not participate in the event asset resolution. Therefore, if an event has its source/target address fall in an invalid device range its asset resolution will not be resolved.
Zone	<ul style="list-style-type: none"> <li>Start address must be less than end address</li> <li>Network zone should not overlap other zones in the same network</li> </ul>	The assets falling within this invalid zone will get invalidated and can not participate in the event asset resolution.
Filter	Dependency constraint. For example, a filter may depend on other resources, like asset, active list, vulnerability etc.	The invalid filter will cause the resources that depend on it to get invalidated.
Rule	Dependency constraint. For example, a rule may depend on other resources, like filter, asset, vulnerability, active list, session list etc.	The invalid rule can not be triggered, so the corresponding correlation events will be missed.

<b>This resource becomes invalid...</b>	<b>when it violates one or more of the following constraints...</b>	<b>which results in...</b>
Data Monitor	Dependency constraint. For example, a data monitor may depend on other resources such as a filter	The invalid data monitor will stop fetching live data to feed the dash board.
Active Channel	Dependency constraint. For example, an active channel may depend on other resources such as a filter, or asset vulnerability	You will not be able to attach or open an invalid active channel
Report	Dependency constraint. For example, a report may depend on other resources, such as filter or asset, vulnerability and active list	The invalid report can not be run either manually from console or as a scheduled task.
Trend	Dependency constraint. For example, a trend that depends on a query will be invalid as soon as a query is changed	The invalid trend will stop generating any trend data.
Scheduled Task	Dependency constraint. For example, a scheduled task may depend on other resources, such as filter	The invalid scheduled task will not run.
Report Template	The report template cannot contain more than 20 charts or more than 15 tables	The invalid template will cause the reports that depend on it to become invalid.
Profile	Dependency constraint. The Profile depends on resources such as the filter it uses to determine which events to run discovery on. It also depends on the group where snapshots and patterns are saved. All these resource must exist and the creator should have appropriate permissions for them.	This resource will get invalidated and the scheduled runs may be skipped.
Active List	If the Active List schema does not match the underlying table etc, or due to some programming error.	The resources (Rules, reports etc.) that are dependent on the Active List get invalidated
Focused Report	Dependency constraint. For example, a focused report may depend on other resources, such as a report, filter or asset.	The invalid focused report can not be run either manually from the Console or as a scheduled task.

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Query	Dependency constraint. For example, a query may depend on other resources, such as a filter, asset, or active list.	The invalid query will cause the resources that depend on it, such as report and trend, to become invalid.

## Automatic and Manual Validation

You can validate individual resource manually through the Console with the **Validate** button as described above.

Resource validation takes place automatically during an upgrade, package import or export, or when you insert or update a resource. (Administrators can use a stand-alone, command-line utility on the Manager machine for validating resources and generating validation reports on an off-line Manager. This is often useful after an upgrade.)

You can validate resources manually either through the Console (as described in [“Fixing and Validating Resources” on page 178](#)) or by running the following command from the `<ARCSIGHT_HOME>/bin` directory on the machine where your ArcSight Manager is installed:

```
arcsight resvalidate -persist [true|false] -excludeTypes <list of comma-delimited resource types>
```



The `resvalidate` is a standalone utility and runs as a batch process. We recommend that you run it only if need be (when there are many database updates that happen offline) after doing a product upgrade only. This utility should not be run while the Manager is running.

After you run this utility, you can find the `validationReport.html` report in the `<ARCSIGHT_HOME>` directory, which will list all the invalid resources.

## Resource Validation During Upgrade

If the Manager detects a conflict during an upgrade or import process, it invalidates the conflicting resource, and continues with the upgrade or import process. The dependent resources for the conflicting resource will be automatically re-validated and disabled after the resource validation process completes.

After an upgrade process, a report called `validationReport.html` is generated in the `<ARCSIGHT_HOME>/upgrade/out/<time-stamp>` directory. After an import process, you can check the Console to make sure that you do not have any invalid resources. You are expected to fix the invalid resources manually. After you resolve the conflict, the dependent resources for the conflicting resource will be automatically re-validated again.

An invalid resource cannot participate in the event flow, trends, reports, data monitors, or channels in real time. For example, if an asset is marked invalid, it cannot participate in the event asset resolution. As a result, correlated events in which the source or target address points to the invalid asset are not generated. Similarly, when a rule is marked invalid, it does not trigger, therefore, the corresponding correlation events will not be generated.

## Extending Audit Event Logging

Starting with ESM v.4.5, updates to existing resources are logged as audit events, as described in “Resources (Configuration Events Common to All Resources)” in the ESM User’s Guide or the Console Help.

If you want to get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property on the ESM Manager to specify which resources should show extended audit event information.

To configure resources for more detailed update auditing, add a URI to the `resource.audit.update.uris` property in the `server.defaults.properties` file. For example:

```
resource.audit.update.uris=/All Users/
```

will turn on extended audit logging for all resources under the `/All Users/` subtree.

Leaving this property blank would turn this feature off (and show only default audit information).

To show detailed audit information for multiple resource types, list resource URIs separated by commas (no spaces). For example, to show extended update audit logging for users and system assets, set the property like this:

```
resource.audit.update.uris=/All Users/,/All Assets/ArcSight System Administration/
```

Extended information on the resource update is logged in two places.

- In the internal audit event generated for the resource update, `Device Custom String5` is set with the update information. The audit event information is shown in the `Device Custom String5` field in this format:

```
<UUID generated for this change>:[<name of attribute>:<old value>:<new value>]+
```

- The update information is also written to a log file, `<ARCSIGHT_HOME>/logs/default/resource_update_audit.log` file. The audit event information is shown in the log in this format::

```
<UUID generated for this change>:<URI of resource>:<ID of resource>:[<name of attribute>:<old value>:<new value>]+
```



- The “+” in the message format examples above is regular expression notation used to indicate that there can be one or more of `<name of attribute>:<old value>:<new value>` triplets shown in the audit event.
- Any “:” character in any attribute name or value is escaped with a backslash to “\:”.
- Any “\” character in any attribute name or value is escaped with a backslash to “\\”.

## Managing Partitions

While the Partition Manager operates automatically, and follows the parameters set for it through the ArcSight Database Configuration Wizard during installation, you can use the Partition features of the Console to review activity and to change partitions’ active, inactive, or reactivated status.



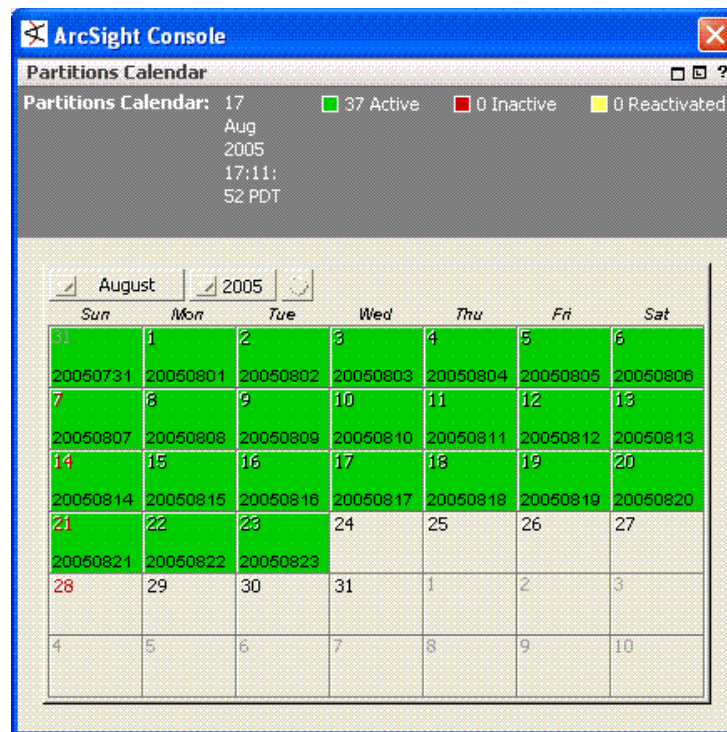
## Getting Partition Information

- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a particular partition.
- 2 Choose **Partition Information**.
- 3 Review the partition's properties as displayed in the Partitions Editor, which are described below.

## Seeing a Partition Schedule

Partition scheduling applies only to the **System Partitions>Active Partitions** branch of the resource tree. The Partitions Calendar graphically shows the partitioning schedule for a group in the Partitions resource tree. This view can help clarify relationships not readily visible in a resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a partition group.
- 2 Choose **Partitions Calendar**.
- 3 View the current schedule or click the **Month** or **Year** selectors to change the time period.



## Archiving Partitions

Archiving a partition removes it from the database and compresses it for long-term storage. Although it may still be stored online, it is offline relative to the database until you reactivate it. Archiving applies only to the System Partitions>Active Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Archive Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to archive and click **OK**.

## Reactivating Archived Partitions

Reactivating a partition restores it to the database, making it available to ArcSight features such as active channels and reports. Reactivation applies only to the System Partitions>Archived Partitions>Inactive Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Reactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

## Reactivating Zipped or Large Archived Partitions

Although you can reactivate most partitions from the Console, follow the process below to reactivate these partitions if

- **Archive Type** was configured as **ZIP** when the partition was archived.
- the partition's **Data Size** field in the Partition Information section of the Partition Editor shows a value of **4000** or greater.

If these conditions are true, do the following:

- 1 Manually unzip the partition with an unzipping tool.
- 2 Ensure that the `arc_event_PartitionName` directory contains the files:

- ◆ `arc_event_data_PartitionName.dmp`
- ◆ `arc_event_data_PartitionName_01.dbf`

If either of these files is missing, the partition archive is invalid and cannot be reactivated. Contact ArcSight Customer Support for assistance.

- 3 On the database machine, enter this in `ARCSIGHT_HOME/bin` to get an SQL interface:

```
arcdbutil sql <username/password>@tnsname
```

- 4 At the SQL prompt, run this script to update the partition's status:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType  
<partition_name>
```

Example:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType 20060101
```

- 5 Check the log `SetPartitionArchiveType.partition_name.log` to ensure that the script ran successfully. The log shows the before and after values for the row corresponding to the partition in the `ARC_PARTITION_SHADOW` table.
- 6 Reactivate the partition from the Console as described above.

## Deactivating Archived Partitions

Deactivating takes a formerly reactivated partition back out of the database. Deactivation applies only to the **System Partitions>Archived Partitions>Reactivated Partitions** branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Deactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

## Running Scheduled Tasks Right Away

You can manually start certain scheduled tasks to cause them to run immediately, rather than wait for the scheduled occurrence. Currently this option covers partition and archive maintenance tasks the system performs automatically.

- 1 Choose the **Partitions** resource tree in the Navigator panel.
- 2 Right-click in the panel and choose **Run scheduled task now**, then **Partition maintenance or Archive maintenance**.
- 3 Depending on the task, timing, and context, the system reports the degree of success or result of the command.

## Partition Properties

Partition Property	Description
Name	The partition's name, usually by date.
Description	A description of the partition.
Lower Bound	The beginning timestamp for the partition.
Upper Bound	The ending timestamp for the partition.
Fully Valid	Indicates whether or not the partitions for all five tables that make up this logical partition checked as valid. These tables are individually validated in the Table Status section below.
Usable	Indicates whether the most important table, Events, is valid.
Active	Indicates whether the partition is accessible to the database (in contrast to "archived").
Archived	Indicates whether the partition has been removed from the database (in contrast to "active").
Event Count	The number of events recorded in the partition.
Data Size (MB)	The number of megabytes of disk space occupied by event data (not indexes).
Index Size (MB)	The number of megabytes of disk space occupied by indexes (not event data).
Index Type	Either default or custom.

Partition Property	Description
Table Status	These five items show the validity status of the partitions for the tables that make up the logical partition. This is summarized in the Fully Valid field above.

## Managing Customers

The Customers resource tree, when populated, maps out the various external or internal customer accounts your enterprise tracks for cost, security analysis, or administrative reasons. These accounts, if present, are usually set up as part of the ArcSight deployment process. If the Customers resource tree is abbreviated or empty, your organization is probably not using this feature.

When the Customers resource tree is populated, you primarily use its branches as references in analysis filters that exclude or include certain customers.

Apart from analysis, the activities necessary to maintain the Customers resource tree include creating new customer references, editing existing references, and occasionally deleting references.

## Creating Customers

When you create a customer, remember that the branch you add to the resource tree has to **match** the Customer URI attribute configured for that branch in the relevant SmartConnectors. In other words, you create customer-tracking resources only for those customers that have parallel URI values set in the SmartConnectors that monitor their devices.

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer group and choose **New Customer**.
- 3 In the Customer Editor, enter values for the properties that identify the customer. Note that the **Name** value has to complete the correct Customer URI for this account as found in its related SmartConnectors.
- 4 Click **Apply** to update the customer and leave the editor open, or OK to complete editing and close the editor.

## Editing Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Edit Customer**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the customer and leave the editor open, or **OK** to complete editing and close the editor.

## Deleting Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Delete Customer**.
- 3 Click **Yes** to confirm the deletion.

## Saving Copies of Read-Only Resources

Although you may be limited to read-only access to certain resources in the Navigator panel, you do have the option to save a copy of such a resource to your own group where you do have write access.

Click the **Save As** button to make a copy of the resource and save it in a specified group.

In the resource group selector dialog, displayed when you click **Save As** in the editor for a read-only resource:

- 1 Select the group in which you want to save a copy of the resource.
- 2 Specify the name you want to assign to your copy of the resource.
- 3 Click **OK**.

The resource copy appears in the resource tree. You have write permission with this copy of the resource.

The Connectors, Users, and Notification editors do not support **Save As** functionality. In these editors, you will see the **OK/Cancel/Apply** buttons, but the fields for those resources are read-only.

## Using the Image Editor

Please contact ArcSight Professional Services for assistance with using this feature.


## Common Resource Attribute Fields

The following fields are common to several types of resources. You can find these fields in the resource editor Attributes tabs for the resources in Common, Assign, Parent Groups, Creation Information, and Last Update Information sections. (See also, [“Resource Attributes” on page 749](#).)

### Common

Entering data in the **Common** section is optional, depending your environment setup.

Field	Description
Resource ID	Read-only field that shows the ArcSight ESM system resource ID.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight ESM. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your ArcSight ESM administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight ESM. A given alias will appear in place of the resource's name everywhere it may be seen. Your ESM administrator can advise you on the correct values for this field, if applicable.  If you use an alternate event naming scheme in your environment, enter an alias for this resource here.

Field	Description
Invalid Reason	<p>If a resource is broken or invalid, an "Invalid Reason" field is included in its Attributes table. An abbreviated explanation is shown in this field. (See also, <a href="#">"Validating Resources" on page 177.</a>)</p> <p>Click the browse button  at the end of this field to get a popup dialog that shows the full text of the explanation.</p>
Description	<p>Description of the resource.</p> <p>You can use this field to communicate the purpose of this resource to other users. For example, if this is a resource that leverages or depends on another resource (e.g., a query viewer or trend that uses an SQL query), this is a good place to make note of that relationship.</p>
Version ID	The globally unique version ID for this resource.
Deprecated	Toggle to indicate whether the resource is current or deprecated (obsolete).

## Assign

Field	Description
Owner	A user selected from the Users resource tree who should be notified about this resource.
Notification Groups	The user groups selected from the Users resource tree who should be notified about this resource.

## Parent Groups

Field	Description
Parent Group	Read-only field that shows the name and path to parent group of this resource.

## Creation Information

Field	Description
Created By	Read-only field that shows the user who created this resource.
Creation Time	Read-only field that shows the date/time when this resource was created.
Time Since Creation	Read-only field that shows the time elapsed since this resource was created. This value is calculated from Creation Time.

## Last Update Information

Field	Description
Last Updated By	Read-only field that shows the user who last updated the resource.
Last Update Time	Read-only field that shows the date/time when this resource was last updated.
Time Since Last Update	Read-only field that shows time elapsed since last update. This value is calculated from Last Update Time.





## Appendix A

# ArcSight Commands

---

This appendix provides information about ArcSight command scripts and utility programs.

## 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.

## Categorized ArcSight Commands

### Archives

`archive` – Import or export resources

`archivefilter` – Manipulate XML resource file

`archivewizard` – Archive wizard

### ArcSight Components

`agents` – Start installed SmartConnectors

`console` – Start the Console

`manager` – Start the Manager

`manager-no-wrapper` – Start the Manager without automatic restart

`managerstop` – Stop the ArcSight Manager

`managerup` – Get the current state of the Manager

`managertreaddump` – Dump threads of the Manager

`webserver` – Start the ArcSight Web server

`webserver-no-wrapper` – Start the Web server without automatic restart

`webserverstop` – Stop the ArcSight Web server

### Certificates

`agent tempca` – Inspect and manage demo certificates for SmartConnectors

`downloadcertificate` – Wizard to import certificate

`keytool` – Manage key stores and trust stores

`keytoolgui` – Graphical tool to manage key stores and trust stores

`listsubjectdns` – Display subject distinguished names from a key store

`tempca` – Inspect and manage demo certificates

### **Configuration**

`agentsetup` – Configure SmartConnectors

`changepassword` – Change passwords in properties files

`consolesetup` – Configure Console

`database pc` – Partition configuration

`managersetup` – Configure Manager

`websetup` – Configure ArcSight Web

### **Database**

`database xts` – Extend database tablespaces

`dbcheck` – Gather information and statistics about the current ArcSight Database instance, primarily for upgrade

### **Event Testing**

`bleep` – Unsupported stress test tool to simulate events (bleepsetup, kickbleep)

`csvconvert` – Create a replay file from a CSV file

`replayfilegen` – Wizard for creating replay files from event data

### **License**

`deploylicense` – Install a new ArcSight license file

### **Logs**

`agent logfu` – Analyze SmartConnector logs

`exceptions` – Search for logged exceptions in logs

`logfu` – Graphical tool to analyze logs or generate log report

`sendlogs` – Wizard to sanitize and send logs to ArcSight for analysis

`threaddumps` – Utility to extract and reformat thread dumps from logs

### **Resources**

`groupconflictingassets` – Group conflicting assets

`managerinventory` – Display configuration information about a Manager

`refcheck` – Resource reference checker

`rescheck` – Verify the integrity of the resource database

### Services

`agentsvc` – Install ArcSight SmartConnector as a service

`managersvc` – Install Manager as a service

`webserver svc` – Install ArcSight Web as a service

### SmartConnectors

`agentcommand` – Send a command (restart, status, terminate) to SmartConnectors

`agent logfu` – Analyze SmartConnector logs

`flexagentwizard` – Generate a simple ArcSight FlexConnector

`regex` – Graphical tool for regex-based FlexConnectors

### Tools

`portinfo` – Display usage information for specific ports

`script` – Run a Python script

`tproc` – Standalone Velocity template processor

`whois` – Lookup an address

### Users

`reenableuser` – Re-enable a user's account

`resetpwd` – Reset a user's password

## Alphabetic List of Commands

### 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>	To retrieve status properties from the SmartConnector:  <code>arcsight agentcommand -c status</code>  To terminate the SmartConnector process:  <code>arcsight agentcommand -c terminate</code>  To re-start the SmartConnector process:  <code>arcsight agentcommand -c restart</code>	

## 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>	To run all SmartConnectors: <code>arcsight agents</code>

## 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>	<div> <div><code>-f file</code></div> <div>Properties file (required in <code>-i</code> silent mode)</div> </div> <div> <div><code>-g</code></div> <div>Generate sample properties file for use in <code>-i</code> silent mode</div> </div> <div> <div><code>-i mode</code></div> <div>Mode: silent, console, swing</div> </div> <div> <div><code>-sn name</code></div> <div>Short Name</div> </div> <div> <div><code>-t type</code></div> <div>SmartConnector Type (overrides short name)</div> </div> <div> <div><code>-w</code></div> <div>Run in wizard mode</div> </div>
<b>Examples</b>	To run the SmartConnector Configuration Wizard: <code>arcsight agentsetup</code>

## 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>	<div> <div><code>-i</code></div> <div>Install the service</div> </div> <div> <div><code>-u</code></div> <div>Run service as user user</div> </div>
<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
<b>Examples</b>	To identify all disabled rules in your current installation:  <code>arcdbutil sql select name from arc_resource where id in (select id from arc_rules where active=0);</code>	
	To get an SQL interface:  <code>arcdbutil sql</code> <code>Enter user-name: / as sysdba</code>	

## 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>	<code>arcdt diagnostic_utility utility_options</code>	
	<code>diagnostic_utility</code>	Utilities you can run are:  <code>runsql</code> —Run SQL commands contained in a file that is specified as a parameter of this utility.  <code>db-alertlog</code> —Retrieve the database alert log from the database machine.  <code>session-waits</code> —Retrieve the currently running JDBC (Java Database Connection) sessions and their wait times.  <code>thread-dumps</code> —Obtain thread dumps from the Manager
<b>Options</b>	<code>utility_options</code>	To see the options available for each utility, run this command in <code>&lt;ARCSIGHT_HOME&gt;\bin:</code>  <code>arcdt help diagnostic_utility</code>
<b>Examples</b>	To find out the number of cases in your ArcSight database:	
	<ol style="list-style-type: none"> <li>1 Create a file called <code>sample.txt</code> in <code>&lt;ARCSIGHT_HOME&gt;/temp</code> on the Manager with this SQL command:  <code>select count(*) from arc_resource where resource_type=7;</code></li> <li>2 Run this command in <code>&lt;ARCSIGHT_HOME&gt;/bin:</code>  <code>arcdt runsql temp/sample.txt</code></li> </ol> <p>To retrieve the last 20 lines of database alert log from your database machine and save it to a file called <code>20060720_dblog</code>, run this command:</p> <p><code>arcdt db-alertlog -ln 20 -o 20060720_dblog</code></p>	

## 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>	
<b>Options</b>	<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> , <code>sort</code> , <code>upgrade</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</code> <code>exportaction</code>	<p>The action attribute to assign to each resource object exported. Export actions are:</p> <p><code>insert</code>: Insert the new resource if it doesn't exist.</p> <p><code>update</code>: Update a resource if it exists.</p> <p><code>remove</code>: Remove a resource if it exists.</p> <p>Default: <code>insert</code></p>
<code>-f archivefile</code>	<p>The input (import) or the output (export) file specification.</p> <p><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</p>
<code>-format fmt</code>	<p>Format of the archive: <code>preferarchive</code>, <code>force</code>, <code>interactive</code>, <code>overwrite</code> or <code>skip</code>. Default: <code>default</code>.</p> <p><code>default</code>: Prompts user to resolve import conflicts.</p> <p><code>force</code>: Conflicts are resolved by the new overwriting the old.</p> <p><code>overwrite</code>: Merges resources, but does not perform any union of relationships.</p> <p><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.</p> <p><code>skip</code>: Do not import resources with conflicts.</p>
<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</code> <code>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</code> <code>excludeTypes</code>	Same as the <code>-xtype</code> option, but will also exclude all references of the specified type
<code>-xuri</code> <code>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</code> <code>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>	Manipulate XML elements and attributes in an archive. The primary use of this command is to exclude system content from a v3.x archive before importing the archive into a v4.0 installation	
<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/.*" 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</code> silent mode)
	<code>-g</code>	Generate sample properties file for <code>-i</code> silent mode
<b>Examples</b>	<p>To change some console configuration options:</p> <pre>arcsight consolesetup</pre>	

## csvconvert

<b>Description</b>	Utility to generate events from a comma-separated values (CSV) file, or to convert events as exported from the event grid into replay file format	
<b>Applies to</b>	Manager, SmartConnectors	
<b>Syntax</b>	<code>csvconvert</code>	
<b>Options</b>	<code>-D file</code>	<b>(Required)</b> Destination file to be created (or extended) in <code>replayagent</code> directory. The convention is to name the file <code>"*.events."</code>
	<code>-h</code>	Display command help
	<code>-s file</code>	Source CSV file
<b>Examples</b>	<p>To run:</p> <pre>arcsight csvconvert -D mystuff.events</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>	To initialize the database
	<code>arcsight database init</code>

## 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: oracle, db2
	<code>-i mode</code>	Mode: silent
	<code>-f file</code>	Properties filename. Required in <code>-i</code> silent mode
	<code>-g</code>	Generate the SQL scripts
	<code>-s</code>	Generate a sample properties file for use in <code>-i</code> silent 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 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>	<div> <div><code>-f fieldset</code></div> <div>URI of the fieldset from which you want to generate the database view</div> </div> <div> <div><code>-m manager</code></div> <div>Name of the Manager</div> </div> <div> <div><code>-n view_name</code></div> <div>Name for the view</div> </div> <div> <div><code>-u user_name</code></div> <div>User name to connect to the Manager</div> </div> <div> <div><code>-p password</code></div> <div>Password for the user_name</div> </div>
<b>Examples</b>	<p>To generate a database view containing fields in the Standard field set:</p> <pre>dbview-generator -f "/All Field Sets/ArcSight System/Active Channels/Standard" -m mymanager -n dv_view_standard -p mypassword -u myuser</pre> <p>To retrieve the data from the view you generated run the following command in SQL:</p> <pre>select * from db_view_standard</pre>

## defaultzones-upgrade

<b>Description</b>	<p>A tool to convert customized <code>defaultZones.csv</code> files for SmartConnectors into network model.</p> <p>This script is required only when you upgrade from v3.0 to v3.5 or later and have customized <code>defaultZones.csv</code> files on your SmartConnectors.</p>
--------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>defaultzones-upgrade [options]</code>	
<b>Options</b>	<code>-source rel_path</code>	<b>(Required)</b> The location of the <code>defaultZones.csv</code> file on your Manager system relative to <code>&lt;ARCSIGHT_HOME&gt;</code>
	<code>-agent agent_identifier</code>	<b>(Required)</b> ID string, the SmartConnector Name, or the SmartConnector's URI.
	OR	OR
	<code>-allagents</code>	Use this option if multiple SmartConnectors share the same <code>defaultZones.csv</code> file.
	<code>-network network</code>	The URI of the network to start with for modeling the networks. (Default: <code>/All Networks/</code> <code>Site Networks/Local</code> )
<b>Examples</b>	<pre>arcsight defaultzones-upgrade -source mydir/defaultZones.csv -agent SF_agent1</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>	<code>deploylicense file</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>	<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>	<code>downloadcertificate</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

---

**Examples**

To run:

```
arcsight downloadcertificate
```

---

## 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] [log files]</code>	
<b>Options</b>	<code>-x element</code>	Exclude element
	<code>-i element</code>	Include element
	<code>-u string</code>	The subject line for notification e-mail
	<code>-e target_email</code>	E-mail address to receive exception notification
	<code>-s host</code>	SMTP server name
	<code>-q</code>	Quiet mode; no printing
	<code>-p</code>	Suppress explanations
	<code>-l</code>	Only show exceptions that have no explanations
	<code>-n</code>	Group unique exceptions
	<code>-r</code>	Exclude errors

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

## 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>

## execprocsvc

Description	Start or stop the Process Executor as a service	
Applies to	Manager	
Syntax	execprocsvc cmd [-wrapperConfig file] [initialHeap maxHeap]	
Options	-c	Console mode
	-i	Install service
	initialHeap	Initial heap memory size, in MB. (Default: 128)
	maxHeap	Maximum heap memory size, in MB. (Default: 512)
	-q	Stop service (quit)
	-r	Remove service
	-s	Start service
	-wrapperConfig file	
Examples	To install a process called 'proc:'	
	arcsight execprocsvc proc -i	
	To run the installed process with a maximum of 1GB of memory:	
	arcsight execprocsvc proc -s 128 1024	

## 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>	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>export_system_tables username/password@TNS name</code>	
<b>Options</b>	<code>username</code>	Oracle database username
	<code>password</code>	Password for the Oracle database user
	<code>TNSname</code>	Name specified in <code>tnsnames.ora</code> for the database from which you are exporting the system tables
<b>Examples</b>	To run: <code>arcsight export_system_tables</code>	

## 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>	

## idefensesetup

<b>Description</b>	Wizard to configure iDefense appliance information on the Manager	
<b>Applies to</b>	Manager	
<b>Syntax</b>	<code>idefensesetup</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	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>import_system_tables export_username import_username import_password TNSname dump_file_path</code>	
<b>Options</b>	<code>export_username</code>	Oracle database username that was used to export system tables using the <code>export_system_tables</code> command.
	<code>import_username</code>	Oracle 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
	<code>dump_file_path</code>	Path name where the <code>arcsight.dmp</code> file is located
<b>Examples</b>	To run: <code>arcsight import_system_tables</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   webkeys   webcerts } (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. ??, 'Kung fu,' means 'work' or 'skill' in Chinese; logfu allows you to practice martial arts on 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 1</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  
managername
```

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 managername
```

To export a package:

#### Examples

```
arcsight package -action export -package "/All  
Packages/Personal/Mypackage" -f packagebundle.arb -u  
username -p password -m managername
```

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 managername
```

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>

To analyze all the queries

```
bin>arcsight querytuner -m analyze
```

To analyze all queries and measure performance if a hint helps, `-t` is the timeout to be used while executing the query:

```
bin>arcsight querytuner -m analyze -t 300000
```

To analyze a single query:

```
bin>arcsight querytuner -m analyze -uri <uri_for_the_query>
```

For example,

```
bin> arcsight querytuner -m analyze -uri "/All
Queries/ArcSight Foundation/Intrusion Monitoring/Executive
Summaries/Business Role/Business Role - Successful Attacks"
```

### Examples

This will tell you if any hint may potentially help. You should see the message "Hint that Helped=<the\_actual\_hint>" in the query-tuner.log file to look for a hint that might potentially help.

Open the `query-tuner.log` file. For every Query at the end of the query report look for the keyword "hasBadPattern=true" followed by "Hint that Helped=<the\_actual\_hint>" or sometimes you will see "No hints could be found for this pattern."

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.

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.

---

**Note:** Please contact ArcSight Customer Support before applying any hints received by running the Query Tuner.

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:

### Applying a Hint to a Query

- 1 In the Console's `<ARCSIGHT_HOME>/current/config/console.properties` file, set the following property:  

```
database.hint.editable=true
```
  - 2 Restart the Console if it is running.
  - 3 Open the `query-tuner.log` file located in the Manager's `<ARCSIGHT_HOME>/logs/` directory.
  - 4 Scan through the file and locate the query URI. Copy the actual hint in the line "Hint that Helped=<the\_actual\_hint>" located below the query URI. Make sure not to copy the words "Hint that Helped="
  - 5 In the ESM Console Navigator, open the **Reports** resource.
  - 6 Click on the **Queries** tab to bring it forward.
  - 7 Follow the URI for the query for which you want to apply the hint, right-click it and select **Edit Query**.
  - 8 In the Inspect/Edit panel, paste the hint you copied in [Step 4](#) in the Database Hint box (the actual hint).
-

## 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 reenabler user &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>Applies to</b>	Manager	
<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>	To run:	
	<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
<b>Examples</b>	To reset a user's password:	
	<code>arcsight resetpwd</code>	

## resvalidate

<b>Description</b>	Utility for checking whether there are any invalid resources in the database. The utility generates two reports called <code>validationReport</code> (with .xml and .html extensions) that are written to the directory from which you run the <code>resvalidate</code> command	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>resvalidate</code>	
<b>Options</b>	<code>-excludeTypes</code>	Resource type to exclude from being checked; for example, Rule, DataMonitor
	<code>&lt;exclude_resource_names&gt;</code>	If specifying multiple resource types to exclude, use comma to separate them.
		Resource type – Rule, DataMonitor(comma separated)
	<code>-out &lt;output_dir&gt;</code>	Output directory for validation report. If none is specified, the report is placed in the directory from which you run the <code>resvalidate</code> command
	<code>-persist [false   true]</code>	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 <code>resvalidate</code> command and <code>-persist=false</code> , the rule will be reported as invalid but not marked invalid. However if <code>-persist=true</code> , the rule will be marked as invalid.
		Default: <code>persist=false</code> .
<b>Examples</b>	To run:  <code>arcsight resvalidate</code>	

## 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>	<code>ruledesc -t {ovo uri} -i info [options]</code>	
<b>Options</b>	<code>-t type</code>	<b>(Required)</b> Type: { ovo   uri }
	<code>-i info</code>	<b>(Required)</b> Info (depends on type).
	<code>-m host</code>	Manager host name or address
	<code>-p pwd</code>	Password
	<code>-port</code>	Port for Manager. Default: 8443

	<code>-prot</code>	Protocol {http   https}. Default: https
	<code>-u name</code>	User name
<b>Examples</b>	To run:	
	<code>arcsight ruledesc</code>	

## runcertutil

<b>Description</b>	A wrapper launcher for the nss certutil tool used for managing certificates and keypairs.  <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.	
<b>Applies to</b>	N/A	
<b>Syntax</b>	<code>arcsight runcertutil</code>	
<b>Options</b>	<code>-A</code>	Add a certificate to the database
	<code>-n</code> <code>&lt;certificate_name&gt;</code>	Alias for the certificate
	<code>-t</code> <code>&lt;trust_attributes&gt;</code>	Set the certificate trust attributes
	<code>-d</code> <code>&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
	<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 keypair to generate
	<code>-x</code>	Self signed
	<code>-m</code> <code>&lt;serial_number&gt;</code>	Certificate serial number
	<code>-v</code> <code>&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>-n &lt;cert_name&gt;</code>	Certificate name
	<code>-H</code>	Help on this tool
<b>Examples</b>	To run: <code>arcsight runcertutil</code>	

## runmodutil

<b>Description</b>	A wrapper launcher for the <code>modutil</code> nss cryptographic module utility.	
<b>Applies to</b>	N/A	
<b>Syntax</b>	<code>arcsight runmodutil</code>	
<b>Options</b>	<code>-fips</code> <code>[true false]</code>	Alias for the certificate
	<code>-dbdir</code> <code>&lt;path_to_directory&gt;</code>	The security database directory
	<code>-H</code>	Help on this tool
<b>Examples</b>	To run: <code>arcsight runmodutil</code>	

## 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.	
<b>Applies to</b>	N/A	
<b>Syntax</b>	<code>arcsight runpk12util</code>	
<b>Options</b>	<code>-d</code> <code>&lt;Certificate_directory&gt;</code>	Path to your certificate directory (nssdb)
	<code>-i</code> <code>&lt;file_to_be_imported&gt;</code>	The name of the file to be imported
	<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>	To run a Python script:	
	<code>arcsight script myScript.py</code>	

## searchindex

	Utility that creates or updates the search index for resources in ArcSight Database.	
<b>Description</b>	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.	
<b>Applies to</b>	Manager, Database	
<b>Syntax</b>	<code>searchindex -a action</code>	
<b>Options</b>	<code>-a action</code>	Possible actions: <code>create</code> , <code>update</code> , or <code>regularupdate</code>  <code>create</code> —Creates a new search index.  <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.  <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.
	<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
	<code>-u user</code>	User name with which to log in to the Manager
<b>Examples</b>	To run:	
	<code>arcsight searchindex -a action</code>	



## 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>	

## startxvfb

<b>Description</b>	Start the X Windows virtual file buffer daemon. (Unix only.)	
<b>Applies to</b>	Manager, Database, Console	
<b>Syntax</b>	<code>startxvfb</code>	
<b>Options</b>	None	
<b>Examples</b>	To start the xvfb daemon:	
	<code>arcsight startxvfb</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)
<b>Examples</b>	To run:	
	<code>arcsight tempca</code>	

## 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
<b>Examples</b>	To run: <code>arcsight tproc</code>	

## 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)</b> <b>&lt;initialHeap&gt;</b> <b>&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 239](#)

[“Query and Trend Performance Tuning” on page 242](#)

[“SmartConnectors” on page 245](#)

[“Console” on page 246](#)

[“Manager” on page 247](#)

[“ArcSight Web” on page 248](#)

[“Database” on page 249](#)

[“SSL” on page 250](#)

## 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.



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.



- 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>\i18n\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.

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 242 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 Oracle 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 with 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.



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 ["querytuner" on page 225](#) (in [ArcSight Commands](#)) 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 249](#).

## 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.

## 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 XP or 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 or **Settings** for Windows XP.
- 3 On Windows XP, select the **Advanced** tab and click **Change**.
- 4 Set **Initial size** to the same value as **Maximum size**.
- 5 Click **Set**.
- 6 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.

## ArcSight Web

### Some content, particularly dashboards, is not visible.

Install the Macromedia Flash plug-in (version 6) to your browser. Visit <http://www.macromedia.com> 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](#), on page 253 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 [Chapter 3, Database Administration](#), on page 71, 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.



# Monitoring Database Attributes

---

This chapter provides information about in-built checks that monitor database attributes and generate warning or error messages, as appropriate.

## 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

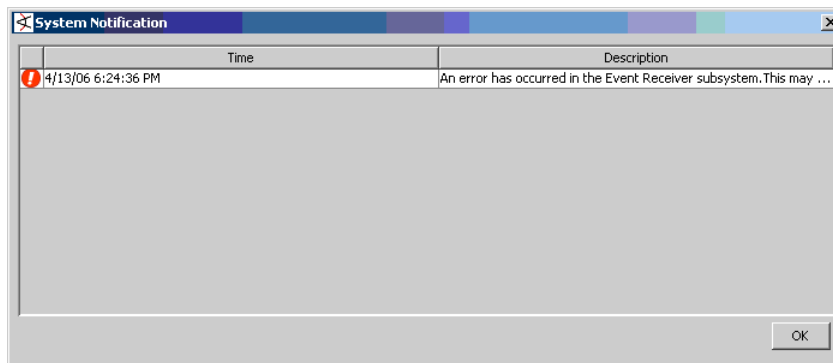
following URL to resume:

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:



## 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.pgaaggreatetarget=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

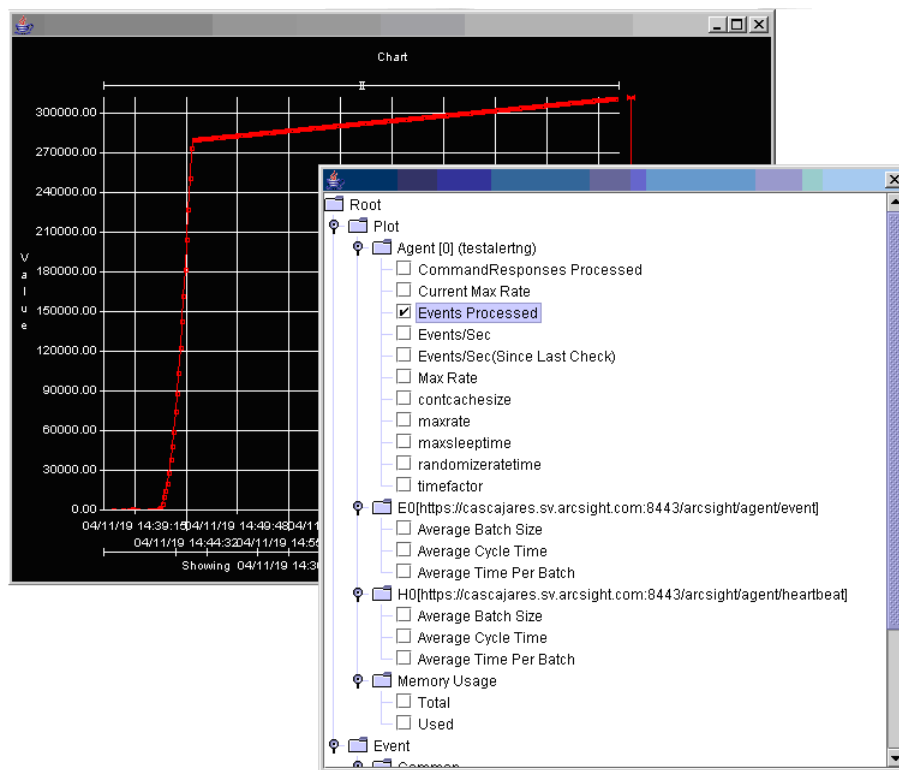
# Partition Manager Error Threshold (# of available reserve partitions)
dbcheck.oracle.manager.errorthreshold=2
```



## Appendix D

# The Logfu Utility

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:

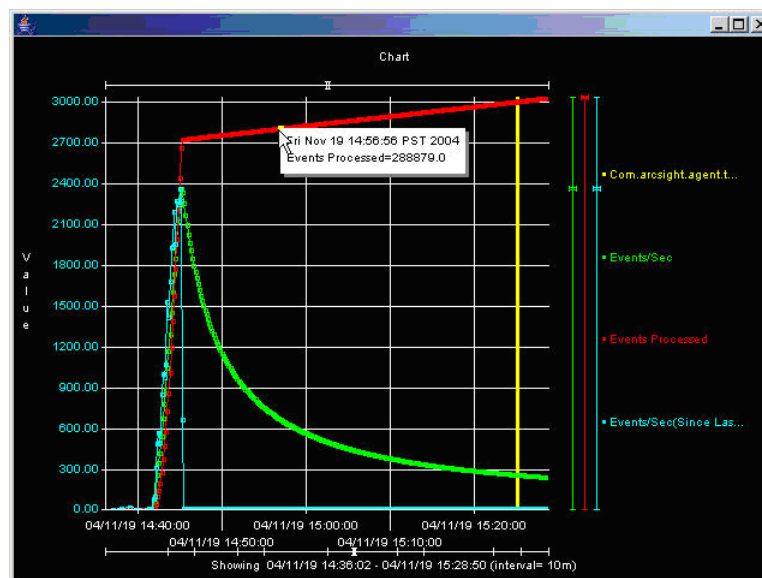
- 1 Open a command window in `<ARCSIGHT_HOME>/logs/default`. This refers to the logs directory under the ArcSight installation directory. (Path separators are / for Unix and \ for Windows.) Logfu requires an X Windows server on Unix platforms.
- 2 Run logfu for the type of log you will analyze:  
  
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.

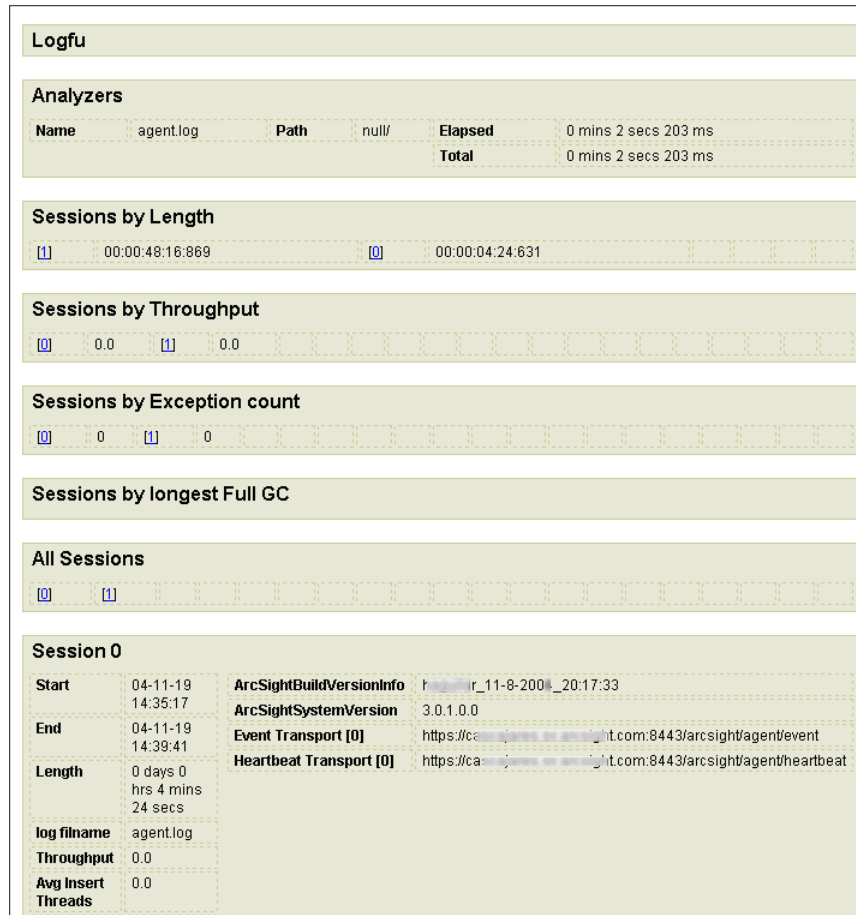
Use the vertical sliders on the right to give each attribute a different scale to keep the peak EPS from the SmartConnector from obscuring the plot of the Manager’s EPS.

## 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).



**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. 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/Short.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 at

<https://mymanager.mycompany.com:9443/arcsight/app?service=external/EventInspector&sp=SfInjoQwBABCGMJkA-a8Z-Q%3D%3D&sp=F&sp=F>

## Appendix F

# The Archive Command Tool

---



Starting with ArcSight ESM v4.0, 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.



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] ...
```



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] ...
```



Both remote and standalone `archive` commands support the same optional arguments.

---

See the description for the `archive` command in [Appendix A, on page 193](#) for more information on this tool.

## Exporting Resources to an Archive

- 1 Open a shell window or a Windows command box, on a computer where either ArcSight Console or ArcSight Manager is installed.



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.



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.



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 box, on a computer where either ArcSight Console or ArcSight Manager is installed.



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.



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 273 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

# Advanced Configuration to Support Standard Content

---

This appendix contains instructions for configuring ArcSight components and standard resources to support the standard content that comes with ArcSight Express.

["Configure SmartConnectors to Send Connector Device Status Events for Critical Devices" on page 279](#)

["Configure Connector Up/Down Resources" on page 280](#)

["Configure Critical Device Not Reporting Resources" on page 281](#)

## Configure SmartConnectors to Send Connector Device Status Events for Critical Devices

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.

The content is based on internal events sent from your SmartConnectors to the ArcSight Manager called Connector Device Status events. These events include the timestamp of the last time the Connector received an event from one of its devices, the count of events sent by a device since the last internal check, and the total count of events sent by a device.

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 ["Managing SmartConnectors" on page 136](#).

## Configure Connector Up/Down Resources

The ArcSight Express content provides the following resources that monitor the operational status of SmartConnectors configured on the ArcSight Express Manager.

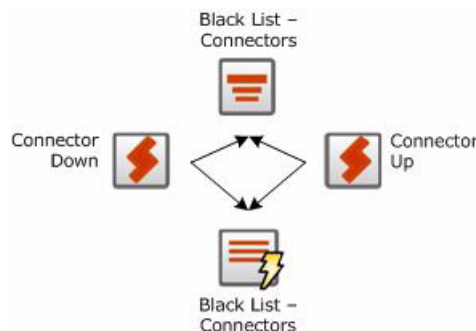
Resource Type	Universal Resource Identifier (URI)	Resource Name
Filter	/All Filters/ArcSight Administration/Connectors/System Health/Custom/	Black List - Connectors
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Down
Rule	/All Rules/ArcSight Administration/Connectors/System Health/	Connector Up
Active List	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/	Black List - Connectors

The rules *Connector Up* and *Connector Down* detect SmartConnectors that are started and reporting events and those that are shut down, and send a notification when Connectors have been down for a certain period of time (by default, 20 minutes).

There may be situations in which you want to exclude certain Connectors from being evaluated by these rules, for example if:

- 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 also reference a filter, which points to the *Black List - Connectors* active list, as shown below.





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.

- 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**. For example:

Name	Value
Connector URI	All Connectors/Site Connectors/Cisco VPN Syslog
Connector Address	111.22.33.0
Creation Time	
Last Modified Time	
Count	1

- 5 Repeat steps 3 and 4 for every SmartConnector you want to exclude from the Connector Up/Down rules.

For more about working with active lists, see the topic *Managing Active Lists* in the *ArcSight ESM User's Guide*.

#### To populate 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**.

## 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

[“Configure SmartConnectors to Send Connector Device Status Events for Critical Devices”](#) on page 279.

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.



- **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 will select 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 also 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 ArcSight Express user. Click **OK**.
- 3 Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.

# Index

---

## A

- About
  - Migrating from one certificate type to another 56
- access control lists
  - for editing user group permissions 85
  - for event permissions 86
  - for operations permissions 84
  - for resource permissions 82
  - for sortable field set permissions 88
- ACLs, *see access control lists*
- action permissions. *See operations.*
- Adjusting
  - Console Memory 12
- administrator
  - tasks, management 75
  - tasks, permissions and resources 81
  - users 81
- alias 189
- Alphabetic List of Commands 196
- arb file
  - see packages*
- archive
  - partitions 185
  - partitions, deactivating 187
  - partitions, reactivating 186
  - partitions, reactivating zipped or large 186
- ArcSight Manager
  - Decoupled Process Execution 2
  - Service Setup on Windows 4
- ArcSight Manager or ArcSight Web Service Setup on Unix Platforms 5
- Asset Categories 96
- asset groups
  - creating 112
- asset ranges
  - CSV file 103
  - populating using wizard 103
- Assets 95
- assets
  - auto-zoning 112
  - creating 108
  - CSV file 101
  - deleting 111
  - editing 111
  - finding 113
  - moving or copying 111
  - populating using wizard 101
  - retrieving vulnerable 115
  - scalability 113
  - showing in a channel 111
- assets groups

- deleting 113
  - editing 112
  - moving or copying 113
  - renaming 112
- attributes, common 189
- auto-zone 112
  - Network Model wizard 105

## B

- Backing up ArcSight Databases 73

## C

- categories
  - grouping assets in 108
- Categorized ArcSight Commands 193
- Changing
  - ArcSight Manager Ports 61
  - Console and ArcSight Web Session Timeouts 61
  - Manager Properties Dynamically 11
  - Oracle Initialization Parameters 72
- Checking Passwords with Regular Expressions 63
- Commonly used elements in Email.vm and Informative.vm files 265
- Comparing Self-signed and CA-signed certificates 31
- Compression and Turbo Modes 65
- Configuring
  - ArcSight Database Monitor 67
  - ArcSight Manager Logging 13
  - ArcSight Manager or ArcSight Web as a Service 4
  - Database Monitor e-mail message recipients 67
  - SNMP trap sender 68
  - the check for free space in Oracle tablespaces 67
- Contents of Email.vm and Informative.vm 266
- customers
  - creating 188
  - deleting 188
  - editing 188
  - managing as a resource 188
- Customizing the template files 268

## D

- data monitors
  - controlling user permissions to deploy 90
  - permissions to deploy 90
- Database Check Tasks
  - List 255
- deprecated 190
- Disabling
  - Database Checks 255

Dynamic Properties 9

## E

Editing

Properties 8

editors

image 189

Enabling

Compression for ArcSight SmartConnector

Events 65

Enforcing Good Password Selection 62

Establishing

SSL Client Authentication with  
Login information 42

Exporting

Resources to an Archive 272

## F

files

adding to packages 128  
creating as resources 126  
deleting 128  
downloading 128  
editing resource attributes 128  
finding 129  
managing as resources 126  
replacing 128  
uploading 126  
viewing 128

filter groups

creating 119  
deleting 120  
editing 120  
moving or copying 120  
renaming 119

filters

creating for SmartConnectors 152  
deleting 119  
editing 118  
exporting, see *packages*  
importing, see *packages*  
moving or copying 119  
SmartConnectors 153

finding

resources in the Console 171

## G

Gathering

logs and diagnostic information 15

graphs

creating to visualize resources 174  
using 174

grid views

for resources 177

groups

assets 112  
filters 119  
notifications 121  
SmartConnectors 162  
vulnerabilities 116

## H

How SSL Works 29

How the Email.vm and Informative.vm

Template Files Work 267

## I

ID

external 189  
resource 189  
version 190

image editor 189

Importing

CA-signed certificate into Manager's key store 38  
Resources from an Archive 273  
v3.x Content to a v4.x ESM System 273

importing and exporting

filters 119  
SmartConnector configurations 164

Installing

New License Files Obtained from ArcSight 13

invalid resource

troubleshooting 180

invalid resources

fixing 178  
overview 177

## K

keytool 28

Keytoolgui 25

## L

locations

describing as assets 108  
editor 109

Logfu

Example 259  
Intervals 263  
Menu 261  
Typical Data Attributes 261

## M

Manager

Password Configuration 62

Managing

and Changing Properties File Settings 8

Migrating

from Demo to CA-Signed 56  
from Demo to Self-Signed 56  
from Self-Signed to CA-Signed 57

model mappings

sending to SmartConnectors 154

Monitoring Available Free Space in Tablespace 73

## N

Network Model wizard

asset CSV file 101  
asset ranges CSV file 103  
auto-zone 105  
column types 98  
using 97

- zone CSV file 100
- Network Modeling
  - Asset Categories 96
  - Assets 95
  - auto zone 105
  - batch loading 97
  - bulk loading 97
  - Networks 96
  - wizard 97
  - Zones 95
- Networks 96
- networks
  - describing as assets 108
  - editor 110
  - sending model mappings to SmartConnectors 154
- Notification Velocity templates 265
- notifications
  - acknowledging, managing received 120
  - categories 120
  - destinations 122
  - e-mail settings 124
  - groups and levels 121
  - inbound 120
  - managing 120
  - pager services 124
  - testing groups and destinations 125
  - wait time settings 125

**O**

- Obtaining
  - CA-signed certificate 37
- operations
  - permissions on 84
  - permissions to deploy data monitors 90
  - setting permissions on 84

**P**

- packages
  - adding files to 128
  - adding resources to 134
  - arb import bundles 132
  - creating 130
  - deleting 134
  - editor 130
  - exporting 133
  - importing 132
  - installing 133
  - managing 129
  - removing resources from 134
  - resolving conflicts 135
  - uninstalling 133
- parent groups 190
- Partition logs 74
- partitions
  - archiving 185
  - deactivating archives 187
  - getting information on 185
  - managing 184
  - properties 187
  - reactivating archives 186
  - reactivating zipped or large archives 186
  - schedules 185
  - schedules, overriding to run tasks now 187

- Password
  - Length 62
  - Uniqueness 64
- passwords
  - changing for user 78
- permissions
  - managing users, user groups 81
- Properties File Settings
  - Defaults and User Properties 8
- Property File Format 8

## Q

- queries
  - for finding resources in Console 172

## R

- Reconfiguring
  - ArcSight Manager 61
  - the ArcSight Console after Installation 60
- Reconnecting to the ArcSight Manager 4
- Reducing Impact of Anti-Virus Scanning 6
- Re-Enabling User Accounts 65
- Removing the ArcSight Manager Service on Windows 5
- reports
  - on vulnerable assets 117
- Requiring Mix of Characters in Passwords 62
- Resetting
  - Oracle Password 73
- resources
  - attributes, common, in editors 189
  - customers 188
  - deprecated 190
  - finding 171
  - fixing 178
  - graphs 174
  - graphs, configuring 176
  - saving copies 189
  - selecting 170
  - sharing 89
  - system core content 92
  - troubleshooting invalid 180
  - validating 177
  - viewing in grids 177
  - visualizing 174
- Restricting Passwords Containing User Name 62
- Restricting the Number of Failed Log Ins 65
- Running
  - ArcSight Command Script 193
  - ArcSight ESM 2
  - Logfu 257

## S

- saving
  - copies of resources 189
- schedules
  - for partitions 185
  - overriding to run partition tasks now 187
- searching
  - for resources 171
  - query options to find resources 172
- Securing
  - ArcSight Manager Properties File 12

- Send Logs utility 14
- Sending
  - Events as SNMP Traps 68
  - logs and diagnostic information to ArcSight 14
- Setting
  - Custom Login Message 3
  - Database Threshold Notification 73
  - Password Expiration 64
- severity
  - setting levels 153
- sharing
  - resources 89
- SmartConnector groups 162
  - creating 163
  - deleting 163, 164
  - editing 163
  - moving or copying 163
  - renaming 163
- SmartConnectors
  - adding filter conditions 153
  - commands 154
  - configuration fields 137
  - configuring 136
  - default Content tab configuration fields 139
  - deleting filter conditions 153
  - editor option tabs 136
  - event severity levels 153
  - exporting configurations 165
  - filters 166
  - filters, creating 152
  - flow-control commands 155
  - getting status 155
  - importing configurations 164
  - network model mappings 154
  - processing categories 151
  - rollback to previous version 169
  - time interval options 152
  - turbo mode 146
  - upgrading 166
- Speeding up partition compression 73
- SSL certificates 31
- Starting
  - and Stopping the ArcSight Manager Service
    - on Windows 4
  - ArcSight Console 3
  - ArcSight Manager 2
  - ArcSight SmartConnectors 3
- Stopping
  - ArcSight Manager 4
- Syntax for Performing Common Archive Tasks 276

## T

- tempca 29
- Terminology
  - SSL Authentication 20
- The #if statement 265
- Tools for SSL configuration 25
- Troubleshooting
  - ArcSight Web 248
  - Console 246
  - Database 249
  - General 239
  - Logfu 259
  - Manager 247

- Partition Archiver problems. 245
- SmartConnectors 245
- SSL 250
- turbo mode
  - on SmartConnectors 146
- Types
  - SSL Certificates 31

## U

- Understanding
  - ArcSight Turbo Modes 66
  - Customization Process 267
  - Database Checks 253
  - SSL Authentication 20
- Unlocking a User-locked Resource 93
- uploading files 126
- user
  - user-created content 92
- user groups
  - ACL edit permissions, deleting 85
  - ACL edit permissions,adding 85
  - creating 80
  - data monitor deploy permissions 90
  - deleting 80
  - editing 80
  - event permissions, adding 86
  - event permissions, deleting 86
  - moving or linking 80
  - operations permissions,adding 84
  - operations permissions,deleting 84
  - renaming 80
  - resource permissions, adding 82
  - resource permissions,deleting 82
  - setting startup views 81
  - sortable field set permissions,adding 88
  - sortable field set permissions,deleting 88
- users
  - access control lists (ACLs) 81
  - creating 76
  - deleting 78
  - editing 78
  - moving or linking 78
  - passwords 76
- Using
  - CA-Signed Certificate 37
  - Certificates to Authenticate Users to ArcSight 59
  - Demo Certificate 32
  - Self-Signed Certificate 33

## V

- validating resources
  - automatic or manual 183
  - overview 177
  - requirements 180
- Verifying
  - SSL Certificate Use 57
- views
  - graph 174
- vulnerabilities
  - describing as assets 108
- vulnerabilities
  - adding an asset to 116
  - creating 114



- deleting 116
- deleting an asset from 116
- editing 115
- editor 110
- moving or copying 115
- vulnerability groups
  - creating 116
  - deleting 117
  - editing 116
  - moving or copying 117
  - renaming 116

## W

- wizards
  - Network Model 97

## Z

- Zones 95
- zones
  - CSV file 100
  - describing as assets 108
  - editor 109
  - populating using wizard 100

