

Administrator's Guide

ArcSight ESM 6.8c

November 18, 2014



Copyright © 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	http://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
11/18/2014	ArcSight ESM Version 6.8	new features

Contents

Chapter 1: Basic Administration Tasks	9
Starting Components	9
Starting the ArcSight Manager	9
Decoupled Process Execution	9
Stopping the ArcSight Manager	10
Starting the ArcSight Console	10
Reconnecting ArcSight Console to the Manager	10
Starting ArcSight Web	10
Starting the ArcSight Command Center	11
Starting ArcSight SmartConnectors	11
Reducing Impact of Anti-Virus Scanning	11
License Tracking and Auditing	11
ArcSight System Tasks	12
Setting up a Custom Login Banner	12
Chapter 2: Configuration	13
Managing and Changing Properties File Settings	13
Property File Format	13
Defaults and User Properties	14
Editing Properties Files	14
Dynamic Properties	15
Example	16
Changing Manager Properties Dynamically	17
Changing the Service Layer Container Port	18
Securing the Manager Properties File	18
Adjusting Console Memory	18
Adjusting Pattern Discovery	19
Improving Annotation Query Performance	19
Installing New License Files Obtained from HP	20
Configuring Manager Logging	20
Sending Logs and Diagnostics to HP Support	21
Guidelines for using the Send Logs utility	21
Gathering logs and diagnostic information	22
Reconfiguring the ArcSight Console after Installation	28

Reconfiguring ArcSight Manager	28
Changing ArcSight Manager Ports	29
Changing ArcSight Web Session Timeouts	29
Managing Password Configuration	29
Enforcing Good Password Selection	30
Password Length	30
Restricting Passwords Containing User Name	30
Password Character Sets	30
Requiring Mix of Characters in Passwords	30
Checking Passwords with Regular Expressions	31
Password Uniqueness	32
Setting Password Expiration	32
Restricting the Number of Failed Log Ins	33
Disabling Inactive User Accounts	33
Re-Enabling User Accounts	33
Advanced Configuration for Asset Auto-Creation	34
Asset Auto-Creation from Scanners in Dynamic Zones	34
Create Asset with either IP Address or Host Name	34
Preserve Previous Assets	35
Changing the Default Naming Scheme	36
Compression and Turbo Modes	37
Compressing SmartConnector Events	37
Reducing Event Fields with Turbo Modes	37
Sending Events as SNMP Traps	38
Configuration of the SNMP trap sender	38
Asset Aging	40
Excluding Assets from Aging	40
Disabling Assets of a Certain Age	40
Deleting an Asset	41
Amortize Model Confidence with Scanned Asset Age	41
Configuring Actors	42
Tuning Guide for Supporting Large Actor Models	43
Permissions Required to Use Actor-Related Data	44
About Exporting Actors	45
Chapter 3: SSL Authentication	47
Terminology	48
How SSL Works	51
Certificate Types	52
SSL Certificate Tasks	53
Export a Key Pair	53
Import a Key Pair	54
Export a Certificate	54

Import a Certificate	55
Creating a keystore	57
Generating a Key Pair	57
Viewing Certificate Details From the Store	57
Delete a Certificate	57
Using a Self-Signed Certificate	58
When clients communicate with one Manager	58
When clients communicate with multiple Managers	60
Using a CA-Signed SSL Certificate	62
Create a Key Pair for a CA-Signed Certificate	62
Send for the CA-Signed Certificate	63
Import the CA Root Certificate	63
Import the CA-Signed Certificate	64
Restart the Manager	66
Accommodating Additional Components	67
Removing a Demo Certificate	67
Replacing an Expired Certificate	67
Establishing SSL Client Authentication	67
Setting up SSL Client-Side Authentication on ArcSight Console	68
Setting up Client-side Authentication on SmartConnectors	75
Migrating from one certificate type to another	77
Migrating from Demo to Self-Signed	77
Migrating from Demo to CA-Signed	77
Migrating from Self-Signed to CA-Signed	77
Verifying SSL Certificate Use	78
Sample output for verifying SSL certificate use	78
Using Certificates to Authenticate Users to ArcSight	79
Using the Certificate Revocation List (CRL)	79
Other Tools for Managing Key- and Truststores	80
keytool	80
tempca	80
Chapter 4: Running the Manager Configuration Wizard	83
Running the Wizard	83
Authentication Details	89
How External Authentication Works	89
Guidelines for Setting Up External Authentication	89
Password Based Authentication	90
Password Based and SSL Client Based Authentication	93
Password Based or SSL Client Based Authentication	93
SSL Client Only Authentication	93

Chapter 5: Managing Resources	95
Appendix A: Administrative Commands	97
ArcSight_Services Command	97
ArcSight Command Index	98
ESM ArcSight Commands	98
Remote Mode	107
Standalone Mode	107
Exporting Resources to an Archive	108
Importing Resources from an Archive	108
Syntax for Performing Common Archive Tasks	109
CORR-Engine ArcSight Commands	134
Appendix B: Troubleshooting	137
General	137
Query and Trend Performance Tuning	139
SmartConnectors	141
ArcSight Console	142
Case data fields appear blank	143
Manager	144
ArcSight Web	144
CORR Engine	145
Temporary sort space limit exceeded	145
SSL	145
Appendix C: The Logfu Utility	149
Running Logfu	150
Example	152
Troubleshooting	152
Menu	154
Typical Data Attributes	154
Intervals	155
Appendix D: Creating Custom E-mails Using Velocity Templates	157
Overview	157
Notification Velocity Templates	157
Commonly Used Elements in Email.vm and Informative.vm Files	158
The #if statement	158
Contents of Email.vm and Informative.vm	158
Using Email.vm and Informative.vm Template Files	159
Understanding the Customization Process	159
Customizing the Template Files	160
Sample Output	161

Index	163
--------------------	------------

Chapter 1

Basic Administration Tasks

This chapter describes tasks you can perform to effectively manage installation or perform additional configuration and maintenance operations for ESM components.

The following topics are covered here:

- ["Starting Components" on page 9](#)
- ["Reducing Impact of Anti-Virus Scanning" on page 11](#)
- ["License Tracking and Auditing" on page 11](#)
- ["ArcSight System Tasks" on page 12](#)
- ["Setting up a Custom Login Banner" on page 12](#)

Starting Components

Start the Manager from a command or console window, or set up the Manager as a daemon. The remainder of this section provides more information about command line options to start, shut down, configure, or reconfigure ESM components. In addition, it provides information about setting up the Manager as a daemon, if you didn't originally configure the Manager that way.

Starting the ArcSight Manager

If the Manager is not configured to run either as a daemon or a service, start it by running the following command as user *arcsight*:

```
/etc/init.d/arcsight_services start manager
```

When you start the Manager as a service, to monitor whether it has successfully loaded, use the command:

```
cd ARCSIGHT_HOME;tail -f logs/default/server.std.log
```

Decoupled Process Execution

On UNIX-based systems, 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. Decoupled process execution uses a stand-alone process executor (instead of using "in process" or "direct process" execution) and sends commands to be executed via the file system. The process executor uses the <ARCSIGHT_HOME>/tmp directory, so restrict system level access for this directory.

The process executor is used, by default, on all Unix platforms. The Manager scripts ensure that the process executor runs as a daemon before the Manager is started. This has some implications with regards to troubleshooting Manager startup and runtime problems. The Manager, if configured to use the process pxeutor, does not start unless it detects the presence of a running process executor. The process executor runs within its own watchdog, like the Manager, so if the process stops for any reason, it restarts automatically. The process executor is transparent to users regarding how the Manager is started or stopped.

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

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

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

Stopping the ArcSight Manager

Stop the Manager service by running the following command as user *arcsight*:

```
/etc/init.d/arcsight_services stop manager
```

Starting the ArcSight Console

To start up the ArcSight Console:

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

```
./arcsight console (on Linux)  
arcsight console (on windows)
```

Reconnecting ArcSight Console to the Manager

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



Note

The connection to the Manager cannot be re-established while the 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 Manager is restarting, or as the connection is re-established.

Starting ArcSight Web

Access the ArcSight Web server through whichever web browser you prefer: Internet Explorer or Firefox. The ArcSight Web home URL is `https://<hostname>:9443/arcsight/app`, where *hostname* is the host name or IP address of the machine on which the web server is running.

Starting the ArcSight Command Center

To start the Command Center from a supported browser enter the following URL:

```
https://<hostname>:8443/
```

Where **<hostname>** is the host name or IP address of the Manager that you specified when you first configured ESM.

Starting ArcSight SmartConnectors

This procedure is just for SmartConnectors that are *not* running as a service. Before you start ArcSight SmartConnectors, make sure the Manager is running. It's also a good idea for the ArcSight Console to also be running, so that you can see the status of the configured SmartConnectors and view messages as they appear on the Console.

To start up an ArcSight SmartConnector:

- 1 Open a command window or terminal box and navigate to the connector's `/current/bin` directory.

- 2 Type in the following line and press **Enter**:

```
./arcsight agents (on Linux)
arcsight agents (on windows)
```

The connector in that folder starts.

Reducing Impact of Anti-Virus Scanning

Files in certain 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:

- It can place a large and constant load on the CPU of the machine.
- It can slow the system down, because frequent scanning can impede writes to disk.

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

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

You may include any directories in `<ARCSIGHT_HOME>` that contain your own files.

License Tracking and Auditing

The system automatically maintains a license audit history that allows you to see how many licenses are in use. When users log into the Console they receive a warning notifying them if they have exceeded their current license. ESM creates an internal audit event for each licensable component to help users track which areas have been exceeded. There are licensing reports on individual features. These reports are located in `/All`

Reports/ArcSight Administration/ESM/Licensing/. The reports provide a summary for the number of Actors, Assets, Users, Devices, and EPS identified over the last week.

ArcSight System Tasks

These system tasks are scheduled to run automatically one or more times per day, depending on the task. You can control some of these schedules indirectly, for example by changing the retention period.

AUP Updater: This task runs in the manager and pushes to connectors any updated AUP packages it might have.

Dependent Resource Validator: This task runs validations on resources in the system and disables the ones that have problems.

PurgeStaleMarkSimilarConfigs: This task does maintenance work on the 'mark similar' annotation criteria, removing the ones that are stale.

Resource Search Index Updater: This task updates the resource search index.

Sortable Fields Updater: This task keeps sortable event fields synchronized, based on the current indices in the database.

Table Stats Updater: This task updates statistics on the non-partitioned schema tables, which includes the resource tables.

Setting up a Custom Login Banner

You can configure the Manager to return a custom login message to display for users logging in to the ArcSight Console.

Set the following property in `server.properties`:

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

This property configures the Manager to send the text from the file

`<ARCSIGHT_HOME>/config/loginbanner.txt` whenever a user runs the ArcSight

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.

Chapter 2

Configuration

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

- [“Managing and Changing Properties File Settings” on page 13](#)
- [“Adjusting Console Memory” on page 18](#)
- [“Adjusting Pattern Discovery” on page 19](#)
- [“Installing New License Files Obtained from HP” on page 20](#)
- [“Configuring Manager Logging” on page 20](#)
- [“Reconfiguring the ArcSight Console after Installation” on page 28](#)
- [“Reconfiguring ArcSight Manager” on page 28](#)
- [“Managing Password Configuration” on page 29](#)
- [“Advanced Configuration for Asset Auto-Creation” on page 34](#)
- [“Compression and Turbo Modes” on page 37](#)
- [“Sending Events as SNMP Traps” on page 38](#)
- [“Asset Aging” on page 40](#)
- [“Configuring Actors” on page 42](#)

Managing and Changing Properties File Settings

Various components 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.

Property File Format

Properties files are text files containing pairs of keys and values. The keys specify the setting to configure. For example, the following property configures the port on which the Manager listens:

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

Blank lines and lines that start with a pound sign (#) are ignored. Use the pound sign for comments.

Defaults and User Properties

Most properties files come in pairs. The first is the defaults properties file, such as `server.defaults.properties`. It contains the default settings. Do not modify these files; use them as a reference. They are overwritten upon upgrade.

The second file is the user properties file, such as `server.properties`. It can contain any properties from the defaults properties file, but the property values in this file override those in the defaults file. Thus, it contains settings that are specific to a particular installation. 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. If an upgrade, such as a service pack or a version update, changes any properties, it does so in the defaults file.

The following table lists the most important properties files.

Default Properties	User Properties	Purpose
<code>config/server.defaults.properties</code>	<code>config/server.properties</code>	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 Files

When you edit a properties file, copy the property to edit from the `*.defaults.properties` to `*.properties` and change the setting to your new value in `*.properties`. When you install an upgrade, and the `*.defaults.properties` file is updated, the properties you customized in `*.properties` remain unchanged.

You can edit the properties using any text editor. Make sure you use one that does not add any characters such as formatting codes.

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 dynamic 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
ICMP	none	ArcSight Console to Target communication (ping tool)
UDP	1645 or 1812	Manager to RADIUS server (if enabled)
TCP	9443	ArcSight Web
	9090	ESM Service Layer Container Port
	9000	Used by the Manager for peering.
TCP	8443	SmartConnector, ArcSight Command Center, and ArcSight Console to Manager communication
TCP	636	Manager to LDAP server (w/ SSL if enabled)
TCP	389	Manager to LDAP server (w/o SSL if enabled)
TCP	143	Manager to IMAP server (for Notifications)
TCP	110	Manager to POP3 server (for Notifications)
UDP/TCP	53	ArcSight Console to DNS Server communication (nslookup tool)
UDP/TCP	43	ArcSight Console to Whois Server communication (whois tool)
TCP	25	Manager to SMTP server (for Notifications)

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 26, 2013, 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.2013_09_26_14_45_27_718
```

On September 27, 2013, 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.2014_09_26_14_45_27_718
```

```
server.properties.2014_09_27_01_05_40_615
```

On September 28, 2014, 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.2014_09_26_14_45_27_718
```

```
server.properties.2014_09_27_01_05_40_615
```

```
server.properties.2014_09_28_03_25_45_312
```

On September 30, 2014, 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.2014_09_26_14_45_27_718
```

```
server.properties.2014_09_27_01_05_40_615
```

```
server.properties.2014_09_28_03_25_45_312
```

The changes made on September 30th are not 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 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, Administrative Commands, on page 97](#).

- 3 Run this command in `<ARCSIGHT_HOME>/bin` to load the new property values:

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

If this command fails with a warning, it means you are changing properties that require a Manager restart. In that case, none of the property changes are applied, including ones that do not require a restart. You can do one of the following in this situation:

- Revert changes to properties that require restarting the Manager and rerun the `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 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` is set to 7, but `search.enabled` continues 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.

Changing the Service Layer Container Port

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

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

- ◆ `/arcsight-dm`
`com.arcsight.dm.plugins.tomcatServer_7.0.21/conf/server.xml`
- ◆ `/config/proxy.rule.xml`
- ◆ `/config/rewriteProxy.rule.xml`

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

- 2 Restart the Manager.

Securing the Manager Properties File

The 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 Manager. Protect the `server.properties` file so that only the user account under which the Manager is running is able to read it. For example, in Unix you can use the `chmod` command:

```
chmod 600 server.properties
```

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

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.sh` configuration file, edit the memory usage range for the Java Virtual Machine.

Adjusting Pattern Discovery

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

- **`patterns.transactionbase.max`** — The maximum transactions allowed in memory. If you exceed this, these transactions are stored as a page file. The default is 10000.
- **`patterns.maxSupporterCost`** — The maximum supporters allowed in memory. If you exceed this number, the Pattern Discovery task aborts. The default is 80000.
- **`patterns.maxUniqueEvents`** — The maximum unique events allowed in memory. If you exceed this number, the Pattern Discovery task aborts. The default is 20000.
- **`patterns.timeSpreadCalculation`** — Set to false avoid calculating timespread statistics, which can take a lot of resources. If you experience performance issues while “Extracting Pattern for Snapshot,” try scheduling Pattern Discovery for off-peak times.

If you run Pattern Discovery against millions of matched events, try reducing the time frame to half to see how long it takes to complete. Use that information to plan when to run it. You can also make the filter condition more granular so there are fewer matches.

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

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

After changing these values, restart the manager for them to take effect.

Improving Annotation Query Performance

If you have annotation queries, their performance can be improved by adding the following property to the Manager’s `server.properties` file:

```
event.annotation.optimization.enabled=true
```

You can edit the properties file using a regular text editor. After adding this property, restart the manager for it to take effect.

Installing New License Files Obtained from HP

You receive new license files packaged as .zip files and sent via e-mail from HP. To deploy the new license file you obtained from HP, please follow the steps below:

- 1 Go to the ArcSight Command Center's **Administration** tab and find the **License Information** section, under **Configuration Management**.
- 2 In the **License File** field specify or browse to the lic or zip file containing the license you want to upload and click **Upload**.
- 3 After uploading, the ArcSight Command Center asks if you want to Restart, which restarts certain ArcSight server processes.

You can choose to restart later. If so, when you are ready, select **Server Management** in the accordion panel under **Configuration Management**, and click **Restart**, at the bottom. You will have to log in again.

If your license has expired and you cannot access a user interface, use the managersetup command, as documented in [“managersetup” on page 120](#).

Configuring Manager Logging

The Manager writes logging information to log files, which by default are located in:

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

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

The number and size of 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 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 affects the number of log files created. The log file currently in use is always the one with no number appended to the name. The log file with the largest number is the oldest. All log files are written to the `<ARCSIGHT_HOME>/logs/default` directory.

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

Log File	Description
<code>server.log*</code>	The main Manager log.
<code>server.status.log*</code>	System status information, such as memory usage etc.

Log File	Description
<code>server.channel.log</code> *	Active Channel logs.
<code>server.std.log*</code>	All output that the Manager prints on the console (if run in command line mode)
<code>server.pulse.log*</code>	The 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 <code>arcsight managersetup</code> utility.

Sending Logs and Diagnostics to HP Support

Customer Support may request log files and other diagnostic information to troubleshoot problems. You can use the Log Retrieval feature in ArcSight Command Center. Check the online help for that feature for more information.

In the ArcSight Console, the Send Logs utility automatically locates the log files and compresses them. You can send the compressed files to Customer Support.

- 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 ESM system, which helps HP Customer Support analyze performance issues on your ESM components.



Note

You can also use the `arcdt` command to run specific diagnostic utilities from the Manager command line. For more information, see [Appendix A, Administrative Commands](#), on page 97.

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

Guidelines for using the Send Logs utility

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

- You can be connected as any valid user on an ESM 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 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 the CORR-Engine. The Send Logs utility only collects logs for the component on which you run it. In order to collect the CORR-Engine logs, the Manager needs to be running.
- All log files for a component are gathered and compressed. That is, you cannot select a subset of log files that the utility should process.

- The Send Logs utility generates a compressed file on your local system that you can send to Customer Support by e-mail, if they request it.
- You can review the compressed file to ensure that only a desired and appropriate amount of information is sent to 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 are removed from the logs.

For example, if you specify 'company.com' as a host-name suffix to remove, the Send Logs utility removes 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 SmartConnectors, 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 ESM components.

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

```
./arcsight agent sendlogs
```

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

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

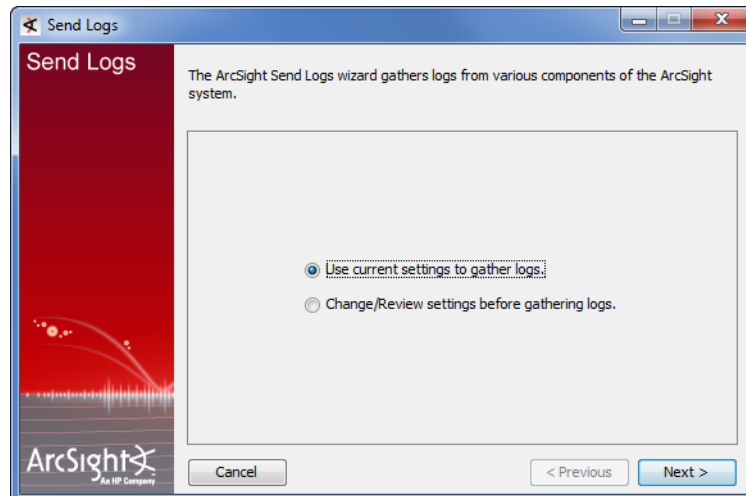
```
./arcsight sendlogs
```

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



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 do not need to re-enter them.

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

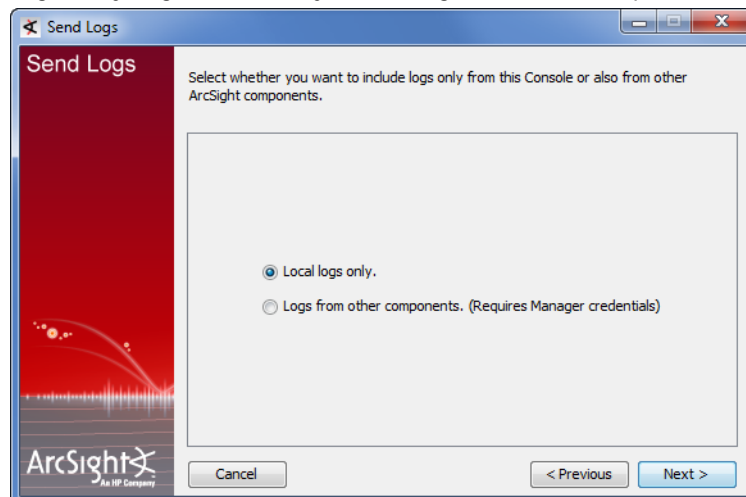


If you select **Use current settings to gather logs**, logs for all components are gathered thus: If this is the first sendlogs is run after installation, then all the logs are gathered. If this is not the first time you have sendlogs has run, it uses the same setting as the previous run.

- a Enter the Manager's login information.
- b Go to the step ["Sanitize logs" on page 26](#).

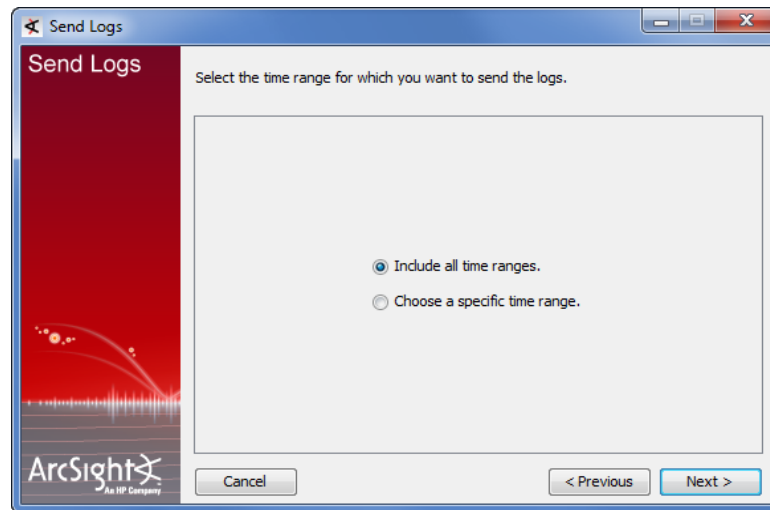
If you selected **Change/Review settings before gathering logs**., you get the option to select the components for which you want logs gathered.

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



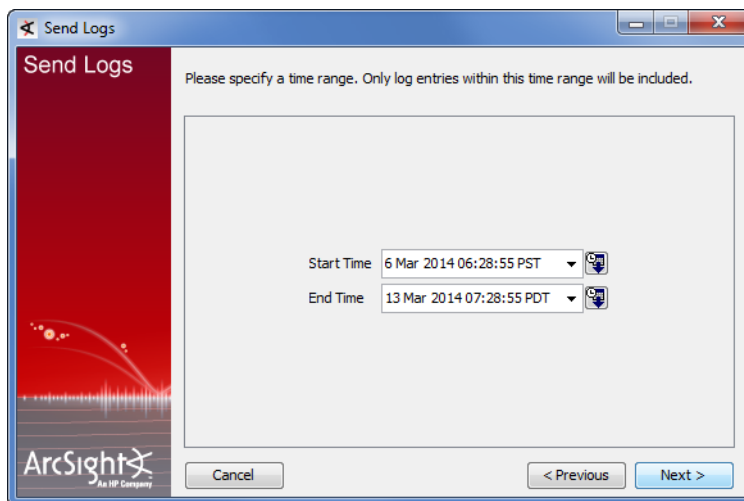
Local logs only:

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



If you selected **Include all time ranges**, go to the step [“Sanitize logs” on page 26](#).

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



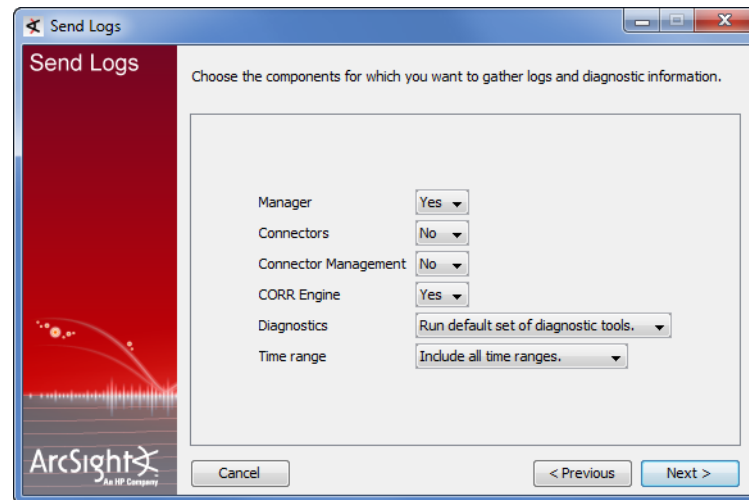
Go to the step [“Sanitize logs” on page 26](#).

Logs from other components (Requires Manager credentials):

If you select **Logs from other components (Requires Manager credentials)**, you are prompted to choose the components.

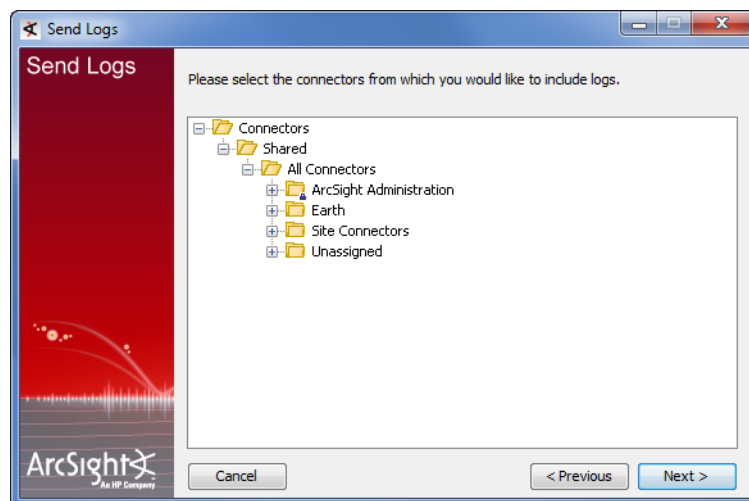
- a** Select the components and the time range for which you want to gather logs. In addition, select whether you want to run the diagnostic utilities to gather additional information for those components. (The options below might be labeled

differently for different versions of this product. For example “CORR-Engine” is “Database” in ESM with Oracle.)



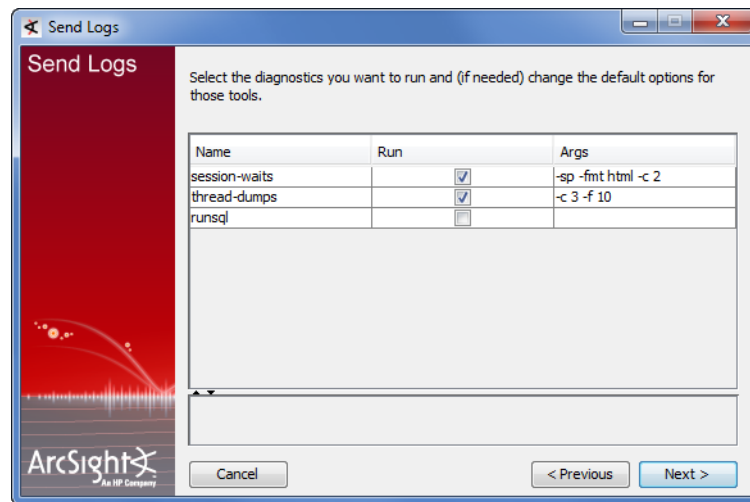
If you choose to specify the diagnostic utilities to run, you are prompted to select the utilities from a list in a later screen. The diagnostic utilities you can select are described in [Appendix A, arcdt, on page 101](#).

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



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

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

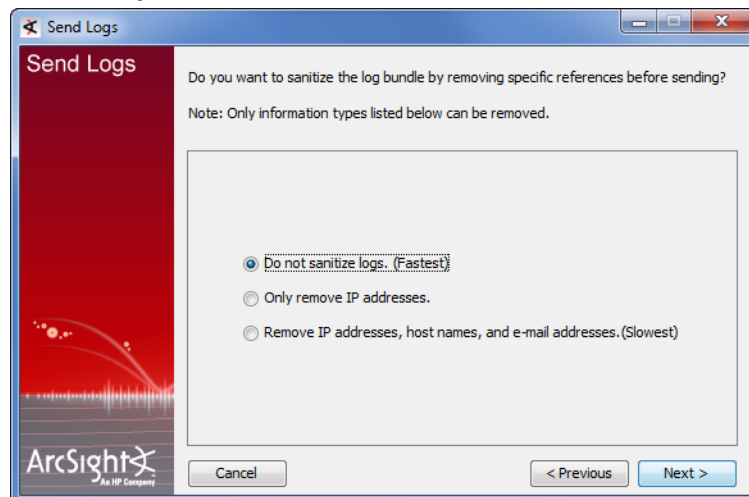


2 Sanitize logs

Select whether you want to sanitize the logs before collecting them. For more information about sanitizing options, see [“Guidelines for using the Send Logs utility” on page 21](#).

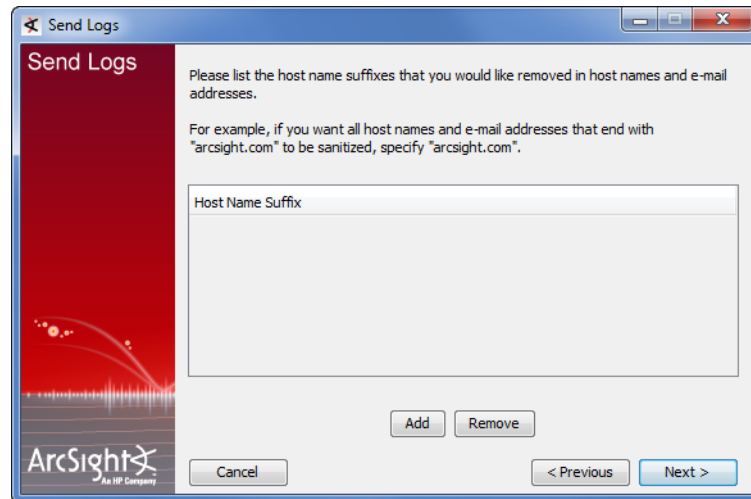
If you choose **Do not sanitization logs (fastest)**, go to the step [“Incident Number” on page 27](#)

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



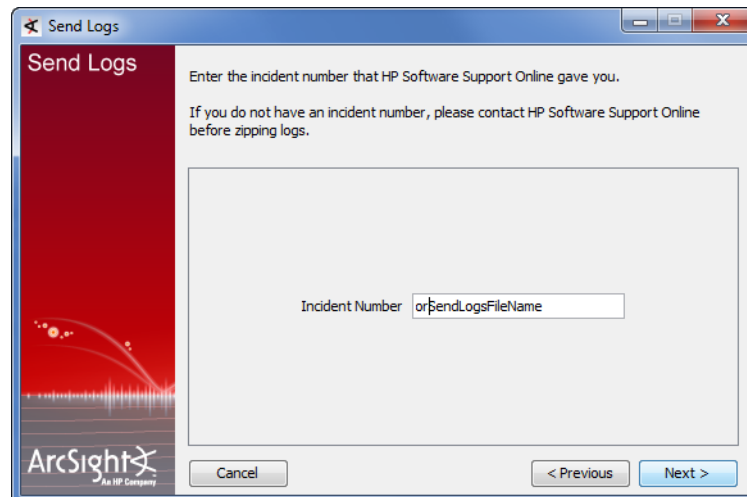
If you chose one of the first two options, go to the step [“Incident Number” on page 27](#).

If you selected **Remove IP addresses, host names, and e-mail addresses (Slowest)**, you are prompted to enter what you want removed. Click **Add** to add a suffix to remove. Highlight an entry and click **Remove** to remove it from the list.



3 Incident Number

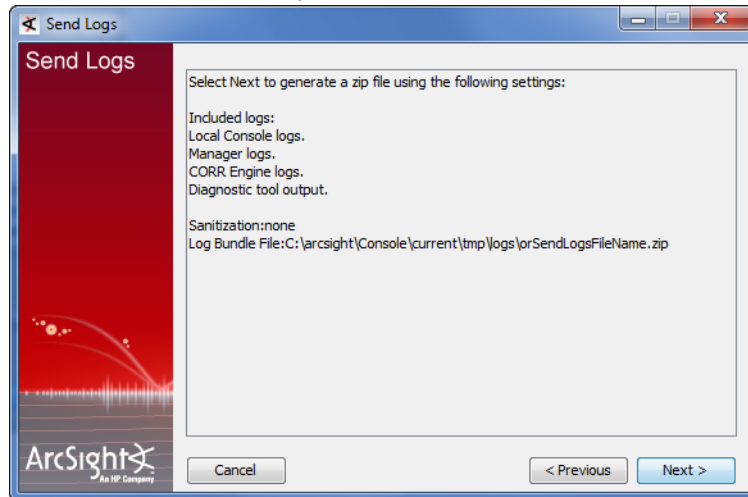
Enter the Customer Support incident number.



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

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

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



Note

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

- 5 Click Done on the final screen.

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

```
./arcsight managersetup
```

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

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

The Manager Configuration Wizard appears to help you re-configure the Manager. The managersetup wizard is covered in [“Running the Manager Configuration Wizard” on page 83](#).

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 Manager is running on. Also, the ArcSight SmartConnectors and ArcSight Consoles must use the same HTTP or HTTPS port numbers the Manager is currently using.

The Manager uses a single port (by default, 8443) that any firewalls between the 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 Manager Configuration Wizard. For more information, refer to the ESM Installation and Configuration Guide.

The Manager also uses port 9000 for the peering feature.

Changing ArcSight Web Session Timeouts

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

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

The ArcSight Web default session timeout can be changed in this file in ArcSight Web's `<ARCSIGHT_HOME>/config/jetty/webserver.xml` file.

In the above .xml files you 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.

Managing Password Configuration

The 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 13](#). Some of these control character restrictions in passwords.

Enforcing Good Password Selection

There are a number of checks that the 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.

Password Character Sets

For appliance users, the Manager comes installed using the UTF-8 character set. If you install the Manager, it allows you to set the character set encoding that the Manager uses.

When you install the ArcSight Console, the operating system on that machine controls the character set the Console uses. Be sure the operating system uses the same character set as the Manager if:

- A user password contains "non-English" characters (in the upper range of the character set: values above 127)
- That user wants to log in with that ArcSight Console.

This is not an issue if you log in from the web-based ArcSight Command Center or ArcSight Web.

For passwords that are in the ASCII range (values up to 127), the character set for the ArcSight Console does not matter.

Requiring Mix of Characters in Passwords

Strong 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, the 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, the 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 \\.

Note

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, the Manager checks all other passwords to make sure nobody is already 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.

Note

Setting Password Expiration

The 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 user names. The passwords of these users never expire.

The 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

The 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, the Manager can be configured to automatically re-enable it after a certain period of time. This reduces administrative overhead, while 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.

Disabling Inactive User Accounts

By default, if a user does not log in for 90 days, the account is automatically disabled. To change the number of days of inactivity before the account is disabled, add the following property to the `server.properties` file:

```
auth.user.account.age=<days>
```

Change `<days>` to the number of days of inactivity allowed before the account is disabled.

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 **Login Enabled** check box for a particular user in the User Inspect/Editor panel in the ArcSight Console.

If the only remaining administrator user account is disabled, a command line tool can be run on the system where the Manager is installed to re-enable user accounts. First, ensure that the Manager is running. Then, from the command line, run the following commands:

```
cd /opt/arcsight/manager/bin
./arcsight reenabler user 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.

Advanced Configuration for Asset Auto-Creation

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

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

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

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

Asset Auto-Creation from Scanners in Dynamic Zones

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

Create Asset with either IP Address or Host Name

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

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

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



Caution

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

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

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

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

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

Preserve Previous Assets

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

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



Caution

Preserving previous assets results in a larger asset model.

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

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

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

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

Changing the Default Naming Scheme

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

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

You can reconfigure this naming scheme. For example, if you want the asset name for an asset in a static zone to appear this way in the ArcSight Console:

myhost_1.1.1.1

In this case, change the default

```
$destinationAddress - $!destinationHostName
```

to

```
$!destinationHostName_$destinationAddress
```

Compression and Turbo Modes

Compressing SmartConnector Events

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

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

```
compression.enabled = false
```

ArcSight SmartConnectors determine whether the Manager they are sending events to supports compression.

Reducing Event Fields with 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, which send fewer event fields from the connector. 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 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.

ESM 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. 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 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 maintains 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.

Sending Events as SNMP Traps

ESM 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 are sent. ESM'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 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 Manager.

The following provides a description of specific SNMP configuration properties:

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

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

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

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

The system uses the filter specified by the URI (it should all be on one line) to decide whether or not an event is forwarded. There is no need to change the URI to another filter.

These contents are locked and are overwritten when the contents are upgraded to the next version. By default, the "SNMP Trap Sender" filter logic is Matches Filter (Correlated Events)—that is, only rules-generated events are 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 depends on your deployment environment and your receiving device. Please consult your receiving device's documentation to find out which community string to use.

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

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

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

The SNMP field types are 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 sends 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 are sent as OCTET STRING.

Asset Aging

The age of an asset is defined as the number of days since it was last scanned or modified. So, for example, if an asset was last modified 29 hours ago, the age of the asset is taken as 1 day and the remaining time (5 hours, in our example) is ignored in the calculation of the asset's age. You can use asset aging to reduce asset confidence level as the time since the last scan increases.



Note

Only the assets belonging to the following categories are considered for aging:

- /Site Asset Categories/Scanned/Open Ports
- /Site Asset Categories/Scanned Vulnerabilities

Excluding Assets from Aging

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

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

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



Note

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

Disabling Assets of a Certain Age

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


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

Deleting an Asset

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

```
# Delete assets when they age

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

Amortize Model Confidence with Scanned Asset Age

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

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

For this example, the value is modified as follows:

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

Asset Age (in days)	AmortizeScan Value
240	0

Configuring Actors

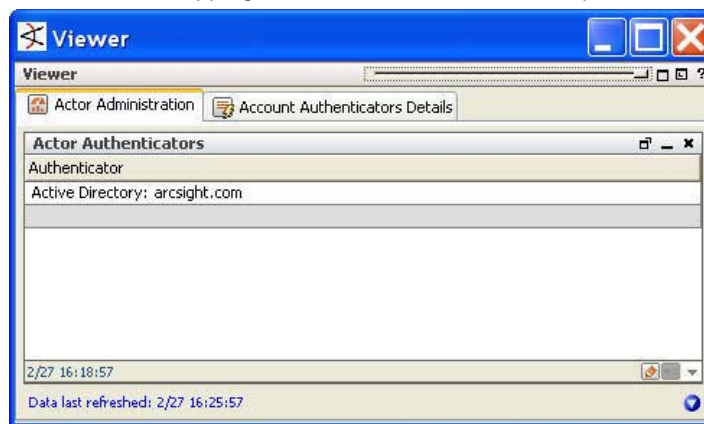
Configuring the Actors feature requires a one-time setup procedure and minimal maintenance if authentication systems are added, modified, or removed from your network. This setup procedure maps the user authentication systems you use in your network environment and the account IDs for each user on those systems.

- 1 Install the Actor Model Import connector appropriate for your IDM.** For complete instructions about how to install the connector, see the relevant SmartConnector installation and configuration guide, such as the SmartConnector Configuration Guide for Microsoft Active Directory Actor Model. Once installed, the connector polls the IDM and imports the user data into the Actor model.
- 2 Identify the authenticators in your environment.** In preparation for configuring the authenticator mapping table, open the dashboard for automatically identifying the user authentication data stores running in your environment and their type:

/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Administration

This dashboard is populated by the following query viewer, which looks for events with a value in the Authenticator field: /All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/Actor Authenticators

The example below shows the value of the Attributes field for an active directory system configured as Active Directory:<domain>.com. Use this exact value, including punctuation, spaces, and capitalization, to populate the account authenticators mapping table described in the next step.



- 3 Configure the Authenticators mapping table.** Using the information gathered in step 2, fill out the account authenticators mapping table provided at /All Active Lists/ArcSight System/Actor Data Support/Account Authenticators. The data you enter here must exactly match the values displayed in the Actor Administration dashboard.
 - In the Navigator panel, go to **Lists > Active Lists**. Right-click the active list /All Active Lists/ArcSight System/Actor Data Support/Account Authenticators and select **Show Entries**.

- b** In the Account Authenticator Details tab in the Viewer screen, click the add icon (+).
- c** For each account authenticator data store, enter the following data:

Column	Description
Device Vendor	The vendor that supplies the authentication data store, such as Microsoft.
Device Product	Provide the application name of the authentication system, such as Active Directory.
Agent Address	The IP address of the reporting SmartConnector.
Agent Zone Resource	The zone in which the reporting SmartConnector resides.
Authenticator	Enter the exact value(s) returned for Authenticator in the Actor Administration dashboard from the previous step, including punctuation, capitalization, and spaces. Using the example shown in the previous step, the value you would enter in this column would be: Active Directory: arcsight.com

When you are finished, the Account Authenticators table should look something like this:

Device Vendor	Device Product	Agent Address	Agent Zone Resource	Authenticator	Creation Time	Last Modified Time	Count
Microsoft	Microsoft Windows	10.10.10.10	<Resource URI="/All Zon...	Active Directory: company.com	14 Apr 2010 17:27:36 PDT	28 Apr 2010 14:27:14 PDT	1
Microsoft	Exchange Server	10.10.10.12	<Resource URI="/All Zon...	Active Directory: company.com	28 Apr 2010 10:42:18 PDT	28 Apr 2010 14:27:23 PDT	1
SAP	Security Audit Log	10.10.10.11	<Resource URI="/All Zon...	Active Directory: company.com	28 Apr 2010 10:41:28 PDT	28 Apr 2010 14:27:29 PDT	1

Tuning Guide for Supporting Large Actor Models

If your actor model contains tens of thousands of members, follow the guidelines in this section to allow adequate processing capacity for best results. If you plan to have between 50,000 and 500,000 actors refer to the Solution Guide for IdentityView 2.5 or later for tuning and configuration information.

- 1 Shut down the Manager.
- 2 **Adjust Java Heap Memory Size in the** `arcsight managersetup` **utility.** Supporting 50,000 actors requires an additional 2 GB of Java heap memory in the Manager. An additional 300 MB is needed for each category model you construct that uses 50,000 actors. This additional memory is not in use all the time, but is needed for certain operations.

For instructions about how to run the `managersetup` utility, see the Installation and Configuration guide.

- 3 Re-start the Manager.
- 4 Proceed with importing the actor model.

For details about starting and stopping the Manager, see [“Starting Components” on page 9](#).

Permissions Required to Use Actor-Related Data

By default, users in the Administrators group have full read/write access to the actors feature and the other resources that actors depend on. The Admin can grant permissions for actors and the other resources upon which the actors feature depends to other users.

To create actors, actor channels, and category models:

- Read and write on /All Actors
- Read and write on /All Session Lists/ArcSight System/Actor Data and /All Session Lists/ArcSight System/Actor Data Support
- Read on /All Field Sets/ArcSight System/Actor Field Sets/Actor Base
- Read on the filters used to define the event ACLS for that user group, for example, All Filters/ArcSight System/Core
- Read and write on the group in which the new resource is being created

To view actors and category models, and monitor actor channels:

- Read on /All actors
- Read on /All Session Lists/ArcSight System/Actor Data and /All Session Lists/ArcSight System/Actor Data Support
- Read on /All Field Sets/ArcSight System/Actor Field Sets/Actor Base

To use actor global variables provided in standard content rules, active channels, and reports that leverage actor data:

Read access on the following resources and groups:

- /All Fields/ArcSight System/Actor Variables (either directly, or inherited from /All Fields/ArcSight System)
- /All Actors
- /All Session Lists/ArcSight System
- /All Active Lists/ArcSight System/Actor Data Support (for the authenticator active list)
- /All Filters/ArcSight Foundation
- The appropriate group that gives all the queries used by a query viewer that leverages actor data
- The appropriate group that contains a query viewer that leverages actor data
- The appropriate group(s) for the filters used by any queries and query viewers that leverage actor data

In addition to these permissions on the actor-related resources themselves, read permissions are needed for any resources (such as filters, user-created actor global variables, and so on) upon which these actor-related resources rely.



Note

Best practice: Log out and log back in again for permission changes to take effect.

As a best practice whenever an admin changes another user's permissions, the other user should log out and log back in again. This ensures that the new permissions are registered with the Manager, and the user can see the changes.

For details about how to assign permissions to user groups, see the ArcSight Console User's Guide topic "Granting and Removing Resource Permissions" in the chapter "Managing Users and Permissions."

About Exporting Actors

If you need to export your entire actor model to image another Manager, you can do it using the `export_system_tables` command-line utility using the `-s` parameter, the parameter used to specify export of session list data. The `-s` parameter captures the special session list infrastructure that is part of the Actor Resource Framework in addition to the actor resources themselves.

For instructions about how to use the `export_system_tables` command-line utility in the chapter "[Administrative Commands](#)" on [page 97](#).

Chapter 3

SSL Authentication

This chapter describes the Secure Socket Layer (SSL) technology used for communication between the Manager and its clients—Console, SmartConnectors, and ArcSight Web. SSL is also used between ArcSight Web and the web browsers that communicate with it, but not between the Manager and the database. This section includes the following topics:

[“Terminology” on page 48](#)
[“How SSL Works” on page 51](#)
[“Certificate Types” on page 52](#)
[“SSL Certificate Tasks” on page 53](#)
[“Using a Self-Signed Certificate” on page 58](#)
[“Using a CA-Signed SSL Certificate” on page 62](#)
[“Replacing an Expired Certificate” on page 67](#)
[“Establishing SSL Client Authentication” on page 67](#)
[“Migrating from one certificate type to another” on page 77](#)
[“Verifying SSL Certificate Use” on page 78](#)
[“Using Certificates to Authenticate Users to ArcSight” on page 79](#)
[“Using the Certificate Revocation List \(CRL\)” on page 79](#)
[“Other Tools for Managing Key- and Truststores” on page 80](#)

SSL enables the Manager 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 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.

Terminology

These terms are used in describing and configuring SSL:

- **Certificate**

A certificate is an entry in the keystore file that contains the public key and 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 51](#).

- **SSL server-SSL client**

An SSL session is set up between two machines—a server and a client. In client-side SSL authentication, the server and its clients authenticate each other before communicating.

The 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.

- **Keystore**

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

Log File	keystore File Name	Location of keystore
Manager	keystore	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webkeystore	<ARCSIGHT_HOME>/config/jetty
Clients[1] (client-side authentication)	keystore.client	<ARCSIGHT_HOME>/config

[1] In client-side authentication, a keystore exists on both the server and the client.

Make sure you do not change the keystore file name.

- **Truststore**

Truststore is an encrypted repository on SSL clients that contains a list of certificates from the issuers that a client trusts. Use the `keytoolgui` utility, to view a truststore.

A certificate is signed by the issuer 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 truststore 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 51](#).

The following table lists the ESM component, the name of the truststore on that component, and its location.

Component	truststore File Name	Location of truststore
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] There are utilities on the Manager machine that are 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 truststores—cacerts for connections to the Manager and webtruststore for connections to browsers.

■ Alias

Certificates and key pairs in a keystore or a truststore are identified by an alias.

■ Truststore password

The `*.defaults.properties` file contains the default truststore password for each ESM component (By default this password is *changeit*). Use a truststore password to encrypt a truststore file. Without this password, you cannot open the truststore file. The password is in clear text. To change or obfuscate it, use the `changepassword` utility, as described in [Appendix A, Administrative Commands, on page 97](#). The following table lists the property name where the obfuscated truststore passwords are stored.

Truststore	Property File	Property Name
Client	<code>client.properties**</code>	<code>ssl.truststore.password</code>
Manager*	<code>server.properties</code>	<code>servletcontainer.jetty311.truststore.password.encrypted</code>
ArcSight Web	<code>webserver.properties</code>	<code>servletcontainer.jetty311.truststore.password.encrypted</code>
Connector	<code>agent.properties**</code>	<code>ssl.truststore.password</code>

*For client-side authentication

** If `config/client.properties` or `user/agent/agent.properties` does not exist, create it using an editor of your choice.

■ Keystore password

Use a keystore password to encrypt the keystore file. Without this password, you cannot open the keystore file. The default is *password* for the Manager and ArcSight Web, and *changeit* for the ArcSight Console's client keystore. The default password for the key pair for any component is the same as for the component's keystore.

You specify a keystore password when creating a key pair, which is discussed in later sections of this chapter. The password is obfuscated and stored in the ESM

component's *.properties file. The following table lists the property name where the obfuscated keystore passwords are stored.

Keystore	Property File	Property Name
Client*	client.properties**	ssl.keystore.password.encrypted
Manager	server.properties	server.privatekey.password.encrypted
ArcSight Web	webserver.properties	server.privatekey.password.encrypted
Connector	agent.properties**	ssl.keystore.password.encrypted

*For client-side authentication

** If config/client.properties or user/agent/agent.properties does not exist, create it using an editor of your choice.

■ NSS database password

The default password for the Manager's nssdb, the Console's nssdb.client, and ArcSight Web's webnssdb are all *changeit*. To change it, see ["Changing the Password for NSS DB" on page 182](#).

■ cacerts

This is the name of the truststore file used for client authentication certificates. There should be a folder with this name on each client machine. There is also one on the Manager machine because there are certain Manager utilities on that machine that communicate with the Manager as clients. The default password for cacerts is *changeit*.

■ Cipher suite

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

The following cipher suites are enabled by default:

- ◆ TLS_RSA_WITH_AES_128_CBC_SHA
- ◆ SSL_RSA_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_RSA_WITH_RC4_128_MD5
- ◆ SSL_RSA_WITH_RC4_128_SHA

Other supported cipher suites are:

- ◆ TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- ◆ TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- ◆ SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_RSA_WITH_DES_CBC_SHA
- ◆ SSL_DHE_RSA_WITH_DES_CBC_SHA
- ◆ SSL_DHE_DSS_WITH_DES_CBC_SHA
- ◆ SSL_RSA_EXPORT_WITH_RC4_40_MD5
- ◆ SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- ◆ SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- ◆ SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

- ◆ SSL_RSA_WITH_NULL_MD5
- ◆ SSL_RSA_WITH_NULL_SHA
- ◆ SSL_DH_anon_WITH_RC4_128_MD5
- ◆ TLS_DH_anon_WITH_AES_128_CBC_SHA
- ◆ SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_DH_anon_WITH_DES_CBC_SHA
- ◆ SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- ◆ SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

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

- ◆ Manager—`config/server.properties`
- ◆ ArcSight Web—`config/webserver.properties`
- ◆ Clients—`config/client.properties`
- ◆ Connectors—`user/agent/agent.properties`

Cipher suites are set as a comma-delimited list in the `ssl.cipher.suites` property. During the SSL handshake, the client provides this list as the 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.

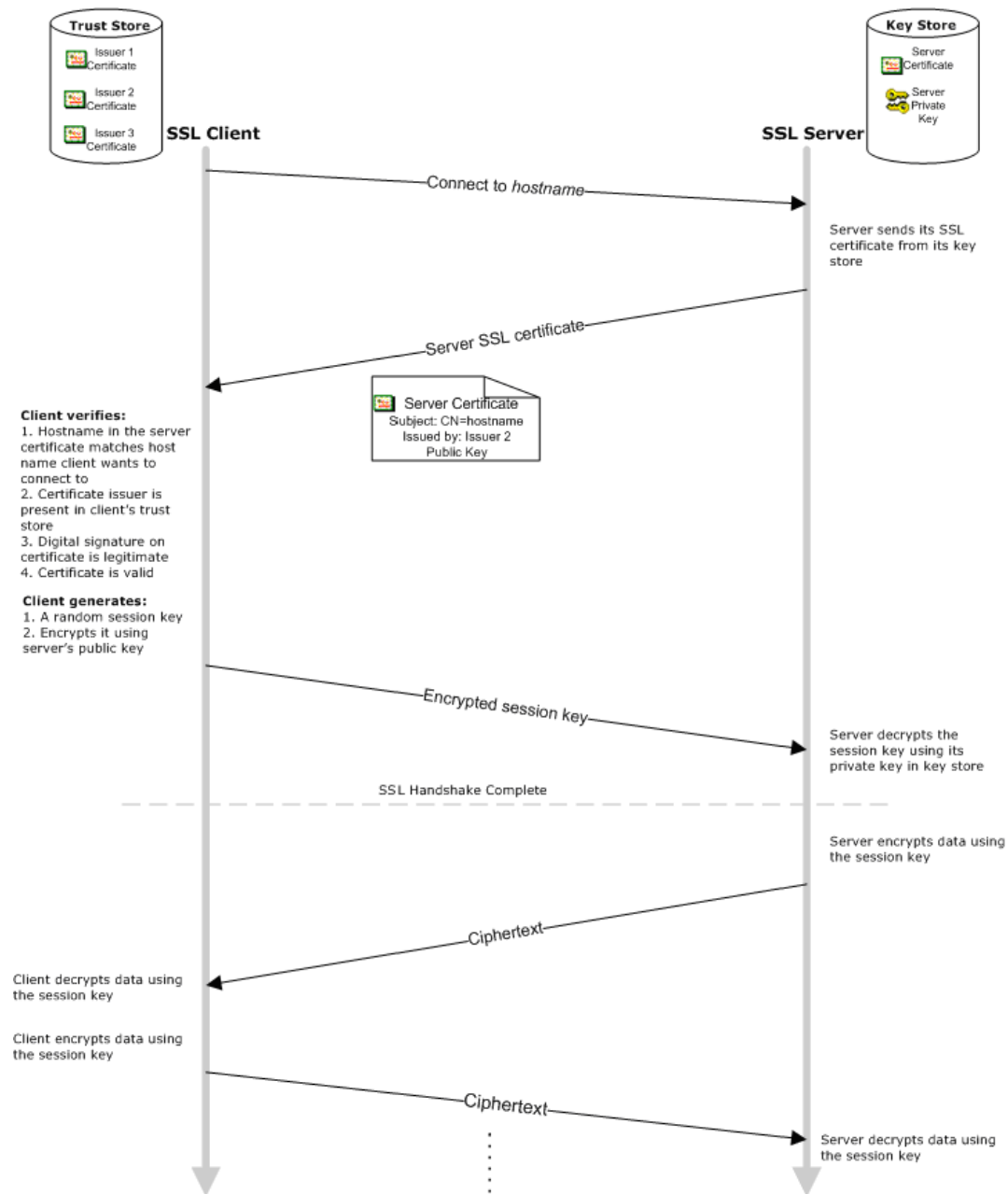
How SSL Works

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 truststore (`<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 truststore.
- 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 following figure illustrates the handshake that occurs between the client and Manager.



With client-side authentication, 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.

Certificate Types

There are three types of SSL certificates:

- CA-signed
- Self-signed
- Demo

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' truststores might already be configured to accept its certificate. Therefore, you may not have to do any configuration on the client side. See ["Using a CA-Signed SSL Certificate" on page 62](#).

You can create your own self-signed certificates. A self-signed certificate is signed using the private key from the certificate itself. Each server is an issuer. Configure clients to trust each self-signed certificate you create.

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

Demo certificates are useful in isolated test environments. Using one in a production environment is not recommended.

SSL Certificate Tasks

The `keytoolgui` utility enables you to perform a number of SSL configuration tasks. The `keytoolgui` utility is available on all components and is located in the `<ARCSIGHT_HOME>/bin/scripts` directory of the component. (To run this tool on Unix, be sure to have X11 enabled.)

To run `keytoolgui`, run this command in `<ARCSIGHT_HOME>/bin`:

```
./arcsight keytoolgui
```

On SmartConnectors, use:

```
./arcsight agent keytoolgui
```

Export a Key Pair

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

```
./arcsight keytoolgui
```
- 2 Click **File->Open keystore** and navigate to the component's keystore.
- 3 Enter the password for the keystore when prompted. For the default password see ["Keystore password" on page 49](#).
- 4 Right-click the key pair and select **Export**.
- 5 Select **Private Key and Certificates** radio button and click **OK**.
- 6 Enter the password for the key pair when prompted. For the default password see ["Keystore password" on page 49](#).
- 7 Enter a new password for the exported key pair file, then confirm it and click **OK**.

- 8 Navigate to the location on your machine to where you want to export the key pair.
- 9 Enter a name for the key pair with a .pfx extension in the Filename text box and click **Export**. You see an Export Successful message.
- 10 Click **OK**.

Import a Key Pair

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

```
./arcsight keytoolgui
```
- 2 Select **File->Open keystore** and navigate to your component's keystore.
- 3 Enter the keystore password when prompted. For the default password see ["Keystore password" on page 49](#).
- 4 Select **Tools->Import Key Pair** and navigate to the location of the key pair file, select it and click **Choose**.
- 5 Enter the password for the key pair file when prompted and click **OK**. For the default password see ["Keystore password" on page 49](#).
- 6 Select the key pair and click **Import**.
- 7 Enter an alias for the key pair and click **OK**.
- 8 Enter a new password for the key pair file to be imported, confirm it, and click **OK**. You see a message saying Key Pair Import Successful.
- 9 Click **OK**.
- 10 Select **File->Save keystore** to save the changes to the keystore and exit the keytoolgui.

Export a Certificate

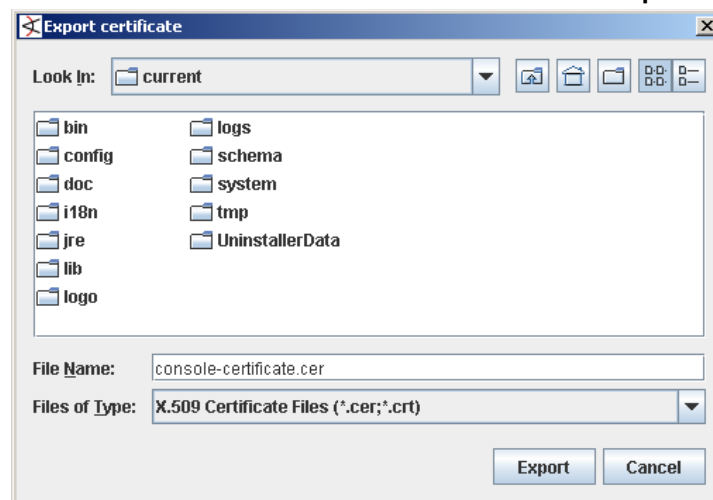
- 1 Start the keytoolgui from the component from which you want to export the certificate. To do so, run the following command from the component's <ARCSIGHT_HOME>/bin directory.

```
./arcsight keytoolgui
```
- 2 Select **File->Open keystore** and navigate to your component's truststore.
- 3 Enter the truststore password when prompted. For the default password see ["Truststore password" on page 49](#).
- 4 Right-click the certificate and select **Export**.

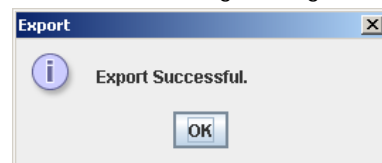
- a** Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- 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 see the following message:



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

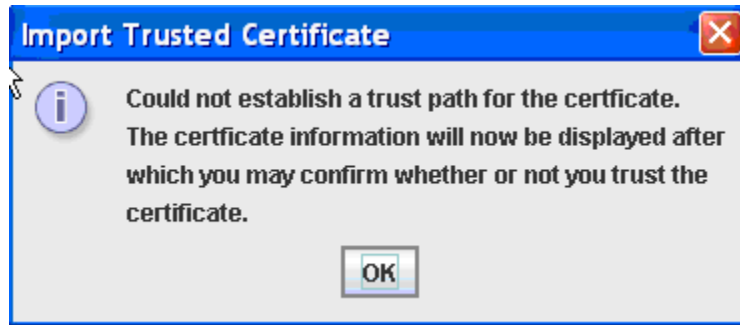
Import a Certificate

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

```
./arcsight keytoolgui
```

- 2** Click **File->Open keystore** and navigate to the truststore (`<ARCSIGHT_HOME>/jre/lib/security`) of the component.

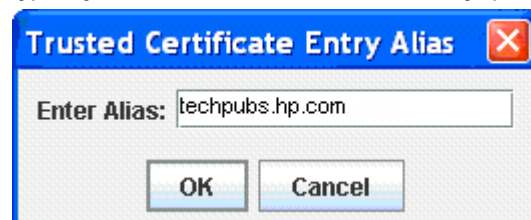
- 3 Select the store named `cacerts` and click **Open**.
- 4 Enter the password for the truststore when prompted. For the default password see ["Truststore password" on page 49](#).
- 5 Click **Tools->Import Trusted Certificate** and navigate to the location of the certificate that you want to import.
- 6 Click **Import**.
- 7 You see the following message. Click **OK**.



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



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



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



- 12 Save the truststore file.

Creating a keystore

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

```
./arcsight keytoolgui
```

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

Generating a Key Pair

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

```
./arcsight keytoolgui
```

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

Viewing Certificate Details From the Store

For certificates in the keystore, truststore, or cacerts, use the keytoolgui command to see certificate information.

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

```
./arcsight keytoolgui
```

- 2 Select **File->Open keystore** and navigate to your component's truststore.
- 3 Enter the truststore password when prompted. For the default password see ["Truststore password" on page 49](#).
- 4 Double-click the certificate whose details you want to view. Details include valid date range, and other information about the certificate.

For the nssdb, nssdb.client, and webnssdb, use the runcertutil command to view certificate information. See ["runcertutil" on page 127](#), for more information.

For the Manager certificate you can also use tempca -i command.

Delete a Certificate

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

Using a Self-Signed Certificate

The procedure you follow depends on the number of Managers with which your clients communicate, because each Manager will have its own self-signed certificate, and any client that has to communicate with different Managers has to be configured to accept all those Manager's certificates.

When clients communicate with one Manager

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

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

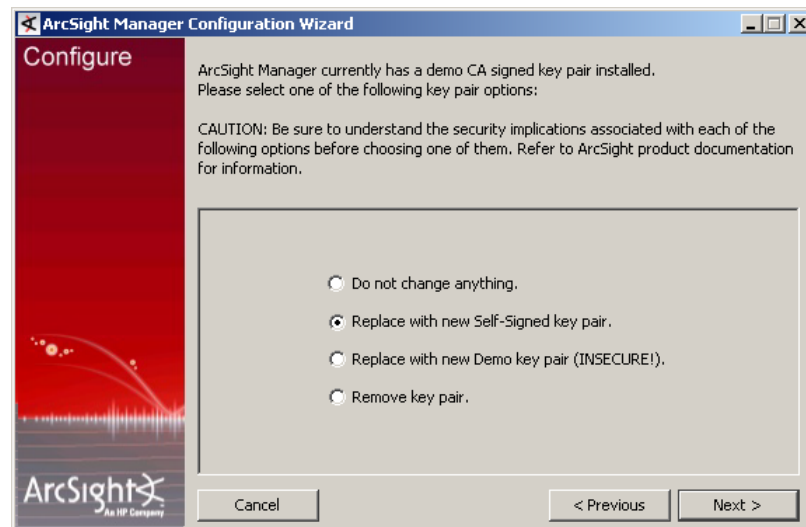


Steps to create a self-signed key pair may be different for a new Manager installation as the Configuration Wizard is launched automatically during the installation process.

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

```
./arcsight managersetup
```

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



- c Enter information about the SSL certificate and click **Next**.

- d Enter the SSL keystore password for the certificate. Click **Next**. Remember this password. You use it to open the keystore.

- e Step through the Configuration Wizard.

The Configuration Wizard does these three SSL-related things:

- It replaces the Manager's keystore at, `<ARCSIGHT_HOME>/config/jetty/keystore`, with the one created using this procedure.
- It generates the `selfsigned.cer` certificate file in the `<ARCSIGHT_HOME>/config/jetty` directory.
- It overwrites the existing Manager truststore file, `<ARCSIGHT_HOME>/jre/lib/security/cacerts`, with one containing the new self-signed certificate to the Manager's truststore file.

The new `cacerts` file contains the information about the Trusted Certificate Authority (CA) that signed your self-signed certificate.

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

- 2 Export the Manager's certificate from
`<ARCSIGHT_HOME>/jre/lib/security/cacerts`.
- 3 Copy the Manager's certificate to each machine from which clients connect to the Manager.
- 4 On those clients, import the Manager's certificate to the
`<ARCSIGHT_HOME>/jre/lib/security` directory. See ["Import a Certificate" on page 55](#).



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

- 5 Restart the Manager process so that the Manager can start using the self-signed certificate.
- 6 Restart all clients.
- 7 When installing a new client, repeat Steps 2-4 of this procedure.
- 8 On the ArcSight Console, perform the steps listed in section ["Setting up SSL Client-Side Authentication on ArcSight Console" on page 68](#).

When clients communicate with multiple Managers

This procedure is for using a self-signed certificate where clients communicate with more than one Manager. In this procedure you get the self-signed certificate files from each manager, copy them to a client, import them all into that client, then copy that client cacerts file to all your other clients.

- 1 Follow [Step 1 on page 58](#) on all Managers. In each case it generates a certificate file called `selfsigned.cer`.
- 2 Copy the `selfsigned.cer` file from each Manager to the
`<ARCSIGHT_HOME>/jre/lib/security` directory on one of your clients.

The certificate files all have the same name. Rename each one so they do not overwrite another on the client. For example, rename the certificate file from ManagerA to `SelfSigned_MgrA.cer`.
- 3 On that client, use the `keytoolgui` utility to import certificates into the truststore (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. For the default password see ["cacerts" on page 50](#).
 - d Click **Tools->Import Trusted Certificate**:
 - i Select the self-signed certificate for a Manager and click **Import**.

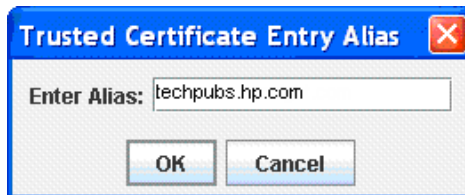
- ii You see the following message. Click **OK**.



The Certificate details are displayed. Click **OK**.

- iii When asked if you want to accept the certificate as trusted, 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 see the following message. Click **OK**.



- vi Save the truststore file (cacerts).
 - 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 Demo certificate:

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

For SmartConnectors, run:

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

- 4** Restart the Manager service so the Manager can start using the self-signed certificate.
- 5** Restart the client.
- 6** Copy the cacerts file to all your other clients and restart them. If you install a new client, copy the cacerts file to it as well.

Using a CA-Signed SSL Certificate

Using certificate signed by a Certificate Authority means replacing your demo or self-signed certificate. Follow the procedure described in this section to obtain and import the certificate to the Manager.

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

- 1 [Create a Key Pair for a CA-Signed Certificate.](#)
- 2 [Send for the CA-Signed Certificate.](#)
- 3 [Import the CA Root Certificate.](#)
- 4 [Import the CA-Signed Certificate.](#)
- 5 [Restart the Manager.](#)
- 6 [Accommodating Additional Components.](#)

Create a Key Pair for a CA-Signed Certificate

To Create a key pair:

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


```
./arcsight keytoolgui
```
- 2 Click **File->New keystore** to create a new keystore.
- 3 Select **JKS** for the keystore Type, it supports Java keystore:
- 4 Click **Tools->Generate Key Pair** to create the key pair. This can take some time.
- 5 Enter key pair information such as 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, used by the clients connecting to this host, can resolve this host name.

For **Email(E)**, provide a valid e-mail address as the CAs typically send an e-mail to this address to renew the certificate.

When you click **OK** it asks you for a new password. Use the password of your existing keystore to save this one. The Manager may fail to start if the password of the Key pair does not match the password of the keystore encrypted in `server.properties`. If

you do not remember the password, run the Manager setup Wizard and change the password of your existing keystore before you proceed. You reuse this file after receiving the reply from the CA.

- 6 Specify an alias name of *mykey* for referring to the new key pair.
- 7 Click **File->Save as** and save the keystore with a name such as `keystore.request`.

For ArcSight Web, save the file with a name such as `webkeystore.request`.

Send for the CA-Signed Certificate

To send for the CA-signed certificate, first create a certificate signing request (CSR).

- 1 In the `keytoolgui` utility, right-click the *mykey* alias name and select **Generate CSR** to create a Certificate Signing Request.
- 2 Choose a path and filename, and click **Generate**.
After you enter a file name, the CSR file is generated in the current working directory.
- 3 Send the CSR to the selected Certificate Authority (CA).

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

Import the CA Root Certificate

When you get the response from the certificate authority, it should include instructions for getting the root CA certificate. You can skip this step if renewing a CA-signed certificate issued by the same root certificate authority. You import the CA root certificate into the truststore file.

- 1 Save the Root CA certificate as a file `rootca.cer`.
- 2 Repeat the following procedure on all the machines where the Manager is installed:
 - a Launch the `keytoolgui` utility on the Manager machine.
 - b Click **File > Open keystore**.
 - c Select the Truststore file located at `<ARCSIGHT_HOME>/jre/lib/security/cacerts`. Use the default password to open `cacerts`. For the default password see ["cacerts" on page 50](#).
 - d Click **Tools > Import Trusted Certificate**, and pick the `rootca.cer` file.
 - e You see the following warning message:
"Could not establish a trust path for the certificate. The certificate information will now be displayed after which you may confirm whether or not you trust the certificate."
 - f Click **OK** to finish.



Note

- If the CA root certificate has a chain, follow the same procedure to import all intermediate CA certificates into the Truststore.
- Update the CA root certificate on other ESM components, as well.
 - Repeat step 2 on one of the Consoles.
 - Copy the updated `cacerts` to any Logger or Connector Appliance, and other machines with Consoles or Connectors.
- Restart all services after the new `cacerts` is copied.

Import the CA-Signed Certificate

When the CA has processed your request, it sends you a file with the signed certificate. You import this certificate into the Manager's keystore.

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 looks similar to this:

```
-----BEGIN CERTIFICATE-----
MIICjTCCAfagAwIBAgIDWnWvMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQT
EiMCAGA1UECBMZrk9SIFRFU1RJTkcGUUVSUE9TRVMgT05MWTEdMBsGA1UEChMUVGhh
d3RlIENlcnRpZmljYXRpb24xZzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQ
QDExNjUaGF3dGUgVGVzdCBDQSBsb290MB4XDTAyMDkyNzIzMzI0MVoXDTAyMTAxODIz
MzI0MVowaDELMAkGA1UEBhMCrVMxDTALBgNVBAGTBGJsYWgxDALBgNVBAcTBGJsYW
gxDALBgNVBAoTBGJsYWgxDALBgNVBAsTBGJsYWgxDALBgNVBAMTFHppZXIuc3Yu
YXJjc2lnaHQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b
+BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vwN4JViC

CSBkDpiqVF7K11Sx4ZVSXX4+VQ6k4gT5G0kDNvQeN05wWkzEMygMB+ZBnYqPA/XtWR
ZtjxvH

MoqS+JEqHruiMLITC6q0reUB/txby6+S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHS
UEDDAKBggrBgEFBQcDATAMBgNVHRMBAG8EAjAAMA0GCSqGSIb3DQEBAUAA4GBAFY3
7E60+P4b3zTLnaG7EVM57GtKE6PwCIilB6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQV
QxnpABjzTalRfYgjNFJ6ltI6ZKjBO5kim9UBeCnKiNNzhIyDyFwbHXOPB/JaLIV+jG
ugYNS7hf/ay0BXKlfue007EgjhhB/mQFs2JB

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

Before proceeding, make sure the name of the issuer that signed your certificate exists as a Trusted CA in cacerts. (Use `keytoolgui` to check your cacerts.)

Follow these steps to import the signed certificate:

- 1 If the returned file has the .CER or .CRT file extension, save it to the `<ARCSIGHT_HOME>/config/jetty` directory and skip to [Step 4 on page 64](#).
- 2 If it has a different extension, use a text editor to copy and paste the text string to a file. Include the lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----", and make sure there are no extra spaces before or after the string.
- 3 Save it to a file named `ca_reply.txt` on the Manager in the `<ARCSIGHT_HOME>/config/jetty` directory.
- 4 On the Manager machine, run this command in `<ARCSIGHT_HOME>/bin`:

```
./arcsight keytoolgui
```
- 5 Click **File->Open keystore** and select the keystore (**keystore.request** or **webkeystore.request**) you saved in [Step 7 on page 63](#). Provide the password you used to save the keystore in that step.
- 6 Right-click the key pair you created at the beginning of the process and named *mykey* in [Step 6 on page 63](#).
- 7 Select **Import CA Reply** from the menu.
- 8 Select the CA reply certificate file you saved in `<ARCSIGHT_HOME>/config/jetty` 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 truststore. 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 keystore named `keystore.request` contains both the private key and the signed certificate (in the alias `mykey`).

- 9 Select **File > Save**. The keystore is now ready for use by the Manager or ArcSight Web.

- 10 Make a backup of the existing keystore by renaming it: Rename `<ARCSIGHT_HOME>/config/jetty/keystore` to `<ARCSIGHT_HOME>/config/jetty/keystore.old`.

If, for any reason, the new keystore does not work properly, you can revert back to the demo keystore you savwed as `keystore.old`.

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

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

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

- 12 For successful reconfiguration and Manager startup, enter the keystore passwords into the appropriate properties file. Enter the password into the `webserver.properties` file for ArcSight Web using the following command (all on one line):

```
arcsight changepassword
-f <ARCSIGHT_HOME>/config/webserver.properties
-p server.privatekey.password
```

Enter the password into the `server.properties` file for the Manager using the following command (all on one line):

```
arcsight changepassword
-f <ARCSIGHT_HOME>/config/server.properties
-p server.privatekey.password
```

After entering this command, the system displays the previous password as asterisks and asks you to enter and then confirm your new password. These commands enter the password into the properties file in an encrypted format.

- 13 If your Manager clients trust the CA that signed your server certificate, go to [“Restart the Manager” on page 66](#).

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



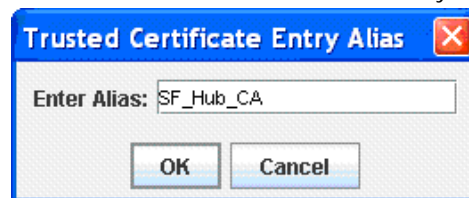
Also perform these steps on the Manager to update the Manager's cacerts so that Manager clients such as the archive utility can work.

- a Obtain a root certificate from the CA that signed your server certificate and copy it to your client machine. (you got this in [“Import the CA Root Certificate” on page 63](#).)
- b For one client, use the `keytoolgui` utility to import the certificate into the truststore (cacerts):

- i In <ARCSIGHT_HOME>/bin, run this command:
`./arcsight keytoolgui`
- ii Click **File->Open keystore**.
- iii Select the store named cacerts. Use the default password to open cacerts. For the default password see ["cacerts" on page 50](#).
- iv Click **Tools->Import Trusted Certificate** and select the certificate you copied in [Step 13, Step a on page 65](#) of this procedure.
- v You 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 truststore and choose **Delete** from the menu.
 - viii Save the keystore.
- c Copy the <ARCSIGHT_HOME>/jre/lib/security/cacerts file from the client in the previous step to all other clients.
- 14** If your ArcSight Web browser clients trust the CA that signed your ArcSight Web certificate, go to [Restart the Manager](#).

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.

Restart the Manager

When you restart the Manager, clients cannot communicate with it until their keystores are populated with the new certificate.

- 1** Restart the Manager.

The Manager may fail to start if the password of the Key pair does not match the password of the keystore, which is encrypted in `server.properties`. If you do not remember the keystore password, run the Manager setup wizard and change the password of your existing keystore.

- 2** Restart all clients.

- 3 To verify that the new certificate is in use:
 - a From the command line navigate to <ARCSIGHT_HOME> and enter the command: `arcsight tempca -i`

The output shows which CA issuer signed the SSL CA-signed certificate, certificate type, status of a validation of the certificate, and so on.
 - b Point a web browser to `https://<manager_hostname>:8443`. to test it.

Accommodating Additional Components

Perform these extra steps to use CA-signed certificates with additional ESM components such as ArcSight Web, the ArcSight Console, or SmartConnectors.

- Adding additional Managers
You do not need to add the CA root certificate to the Truststore-cacerts file again. Just copy the cacerts file from the existing Manager to the new Manager.
- Other ArcSight Components (Console, ArcSight Web, and SmartConnectors).
When installing a new Console, copy the cacerts file from an existing Console to the new Console.

Removing a Demo Certificate

You can remove the demo certificate by using the tempca script located in <ARCSIGHT_HOME>/bin. Issue the following command on all Manager and Console installations:

```
arcsight tempca -rc
```

For SmartConnectors, run the tempca script using the following command:

```
arcsight agent tempca -rc
```

Replacing an Expired Certificate

When a certificate in your truststore/cacerts expires, replace it with a new one as follows:

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

To delete a certificate from the truststore/cacerts, start `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. Use `keytoolgui` to import the new certificate into the truststore/cacerts. See [“Using a Self-Signed Certificate” on page 58](#), or [“Using a CA-Signed SSL Certificate” on page 62](#) section (depending on the type of certificate you are importing) for steps on how to import the certificate.

Since the common name (CN) for the new certificate is the same as the old certificate, you cannot have both of them in the truststore, cacerts.

Establishing SSL Client Authentication

By default, clients (SmartConnectors, Consoles, and ArcSight Web) authenticate using user name and password. The clients can optionally use SSL authentication for clients. If SSL

client authentication is enabled, you can optionally disable user name and password login, as described in the next section.

When client-side authentication is used, the SSL clients contain a keystore and the SSL server contains a truststore.



Note

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

Setting up SSL Client-Side Authentication on ArcSight Console

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 these steps:
 - 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 opens the New keystore Type dialog.
- c** Select **JKS** and click **OK**.

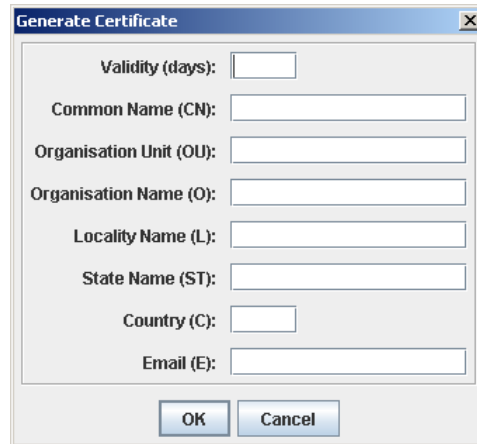


- d** Click **Tools->Generate Key Pair** and fill in the fields in the following dialog:

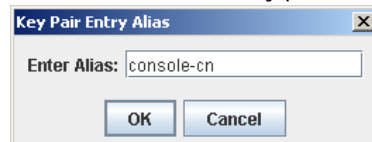


Note

The Common Name field in the following screen should be the external ID of the user logging in to the Manager that this console connects to.

A Java-style dialog box titled "Generate Certificate" with a close button (X) in the top right corner. It contains several text input fields for certificate details: "Validity (days):", "Common Name (CN):", "Organisation Unit (OU):", "Organisation Name (O):", "Locality Name (L):", "State Name (ST):", "Country (C):", and "Email (E):". At the bottom are "OK" and "Cancel" buttons.

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

A Java-style dialog box titled "Key Pair Entry Alias" with a close button (X) in the top right corner. It contains a single text input field labeled "Enter Alias:" with the text "console-cn" entered. At the bottom are "OK" and "Cancel" buttons.

Caution

If you plan to install the Console, Manager, and Web on the same machine, make sure that this alias is unique. Also, do not 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.

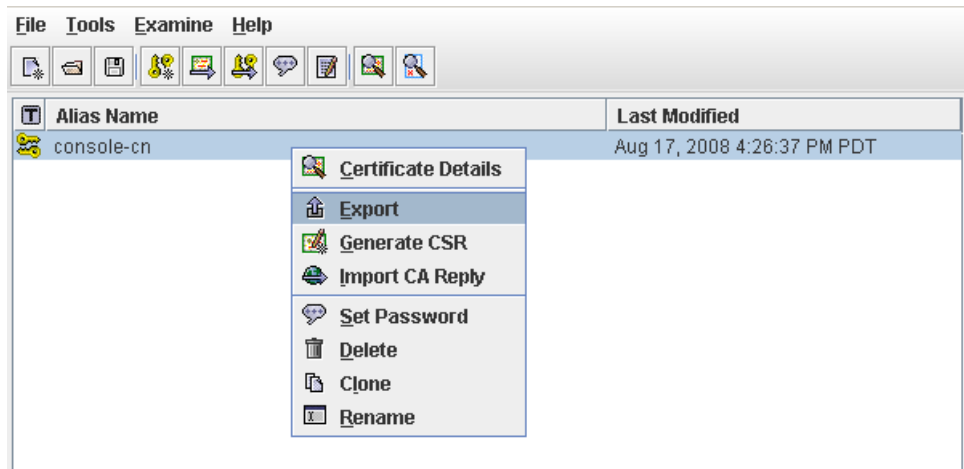
When you install ArcSight Web, set the CN of the ArcSight Web's key pair you generate to the name or IP address of the machine on which you are installing it. Hence, if both Web and Console are on the same machine, and if you use the machine name or IP address for the CN for both the Web and the Console,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

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

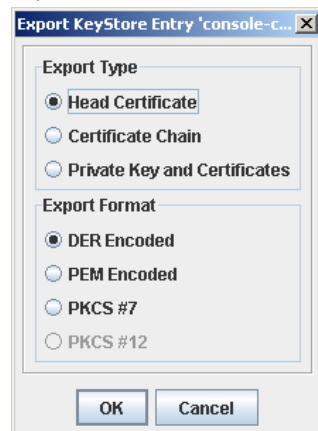
A Java-style dialog box titled "Key Pair Entry Password" with a close button (X) in the top right corner. It contains two text input fields: "Enter New Password:" and "Confirm New Password:". At the bottom are "OK" and "Cancel" buttons.

- 2 Export the key pair you just generated.

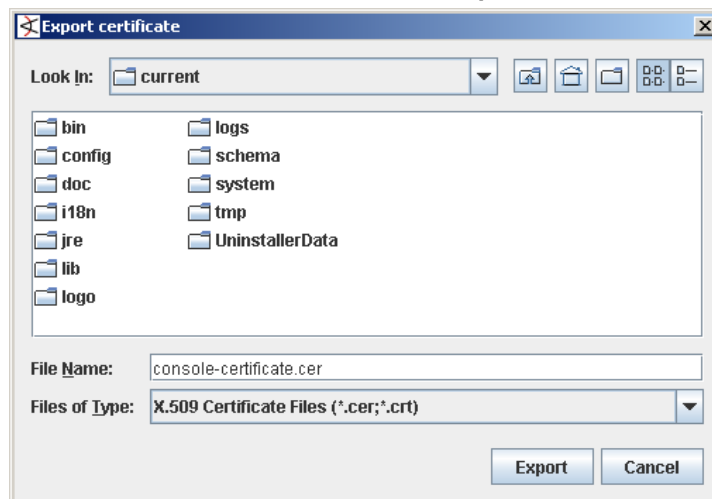
- a** In keytoolgui, right-click the key pair you just generated and select **Export**.



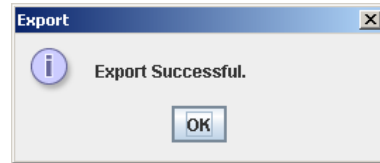
- b** Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



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



- d You 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.

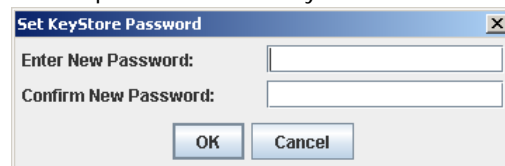
Import the signed certificate response in the keystore of all Consoles.

- ◆ Import the signed certificate response in the Console's keystore, `keystore.client`. Follow the steps in section ["Import the CA Root Certificate" on page 63](#).
- ◆ Use the `changepassword` tool to set an encrypted keystore password in the `client.properties` file:

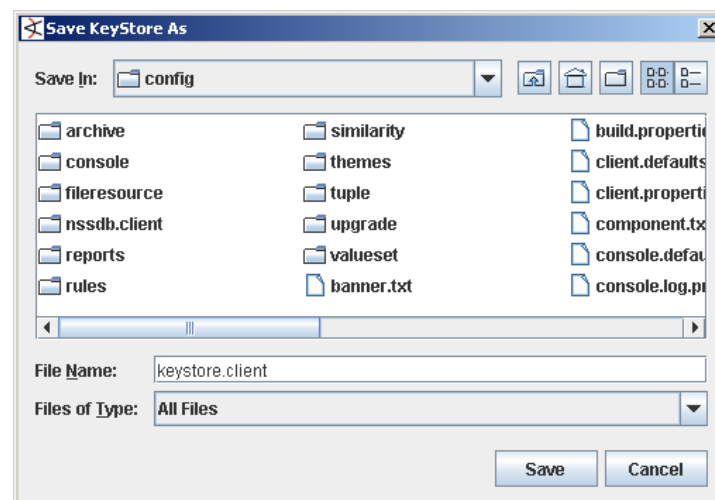
```
arcsight changepassword -f config/client.properties -p
ssl.keystore.password
```

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

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



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



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

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

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

The `ssl.client.auth` property should already be set correctly:

```
ssl.client.auth=true
for "password-based and SSL client-based authentication"
```

```
ssl.client.auth=true
for "SSL client only authentication"
```

```
ssl.client.auth=optional
for "password-based or SSL client-based authentication"
```

Do not change the keystore name to anything other than `keystore.client`

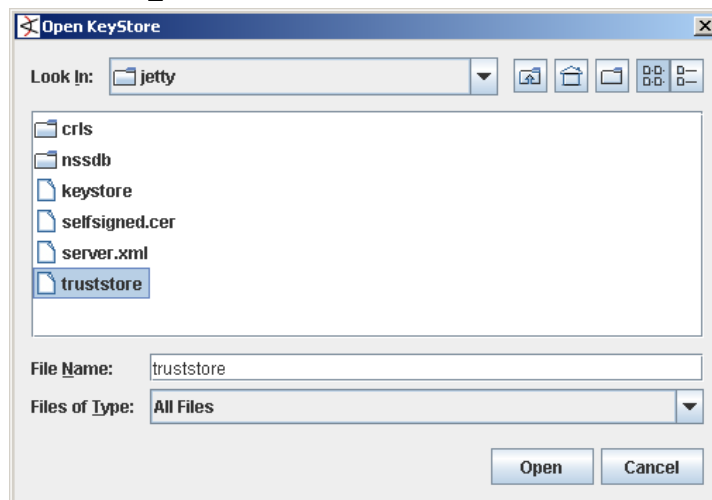
- 6 Use the `changepassword` tool to set an encrypted keystore password in the `client.properties` file:

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

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

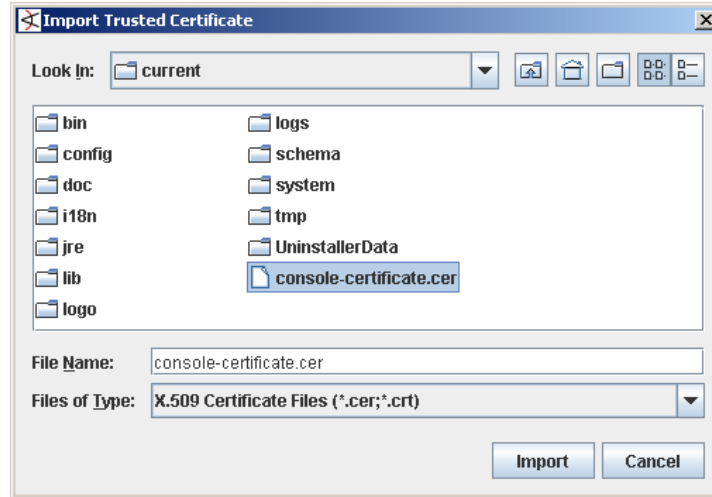
If your Manager trusts the CA that signed your Console's certificates, go to the next step. Otherwise perform these steps to update the Manager's truststore.

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



- c Enter *changeit* when prompted for the truststore 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 see the following message. Click **OK**.



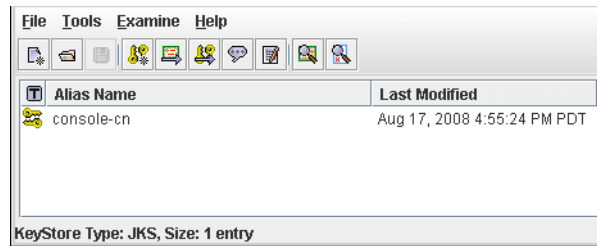
- g Review the certificate details and click **OK**.
- h For “**Do you want to accept the certificate as trusted?**” Click **Yes**.
- i Enter an alias for the certificate.



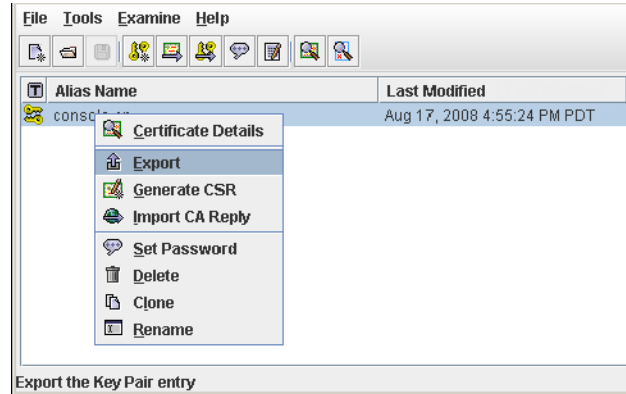
- j Click **OK** and save the changes to the truststore.

- 8 Stop the Manager as user *arcsight* by running:
- ```
/etc/init.d/arcsight_services stop manager
```
- 9 From the `/opt/arcsight/manager/bin` directory, run:
- ```
./arcsight managersetup
```
- 10 Change the SSL selection to the appropriate setting. You can leave all the other values as they were and finish the configuration wizard.
- 11 Restart the Manager service.
- 12 Restart ArcSight Console.
- 13 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.

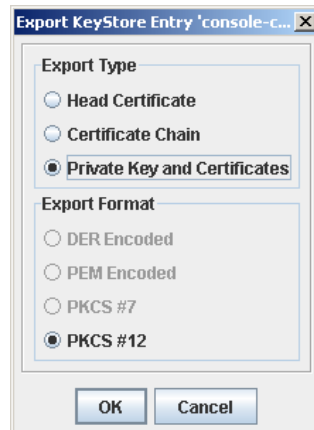
- b Click on **File->Open keystore** and navigate to the Console keystore you created.



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

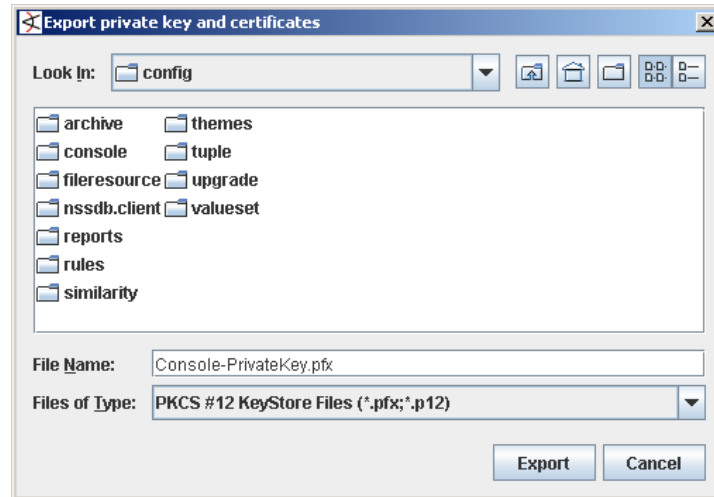


- d Select **Private Key and Certificates** as Export Type and **PKCS#12** as the Export Format if not already selected and click **OK**.



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

- g Enter a name for the Console's private key with a .pfx extension and click **Export**.



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

- 14 Exit keytoolgui.

Setting up Client-side Authentication on SmartConnectors

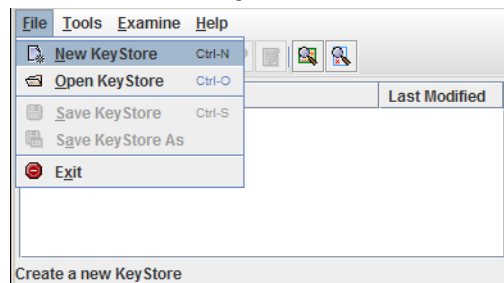
In order to enable client-side authentication on clients (SmartConnectors) running in default mode, perform these steps:

- 1 Create a new client keystore in the SmartConnector's `/config` directory.
 - a Start the keytoolgui from the client's `bin` directory by running the following:

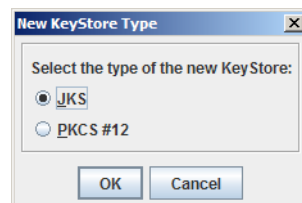
On SmartConnector:

```
./arcsight agent keytoolgui
```

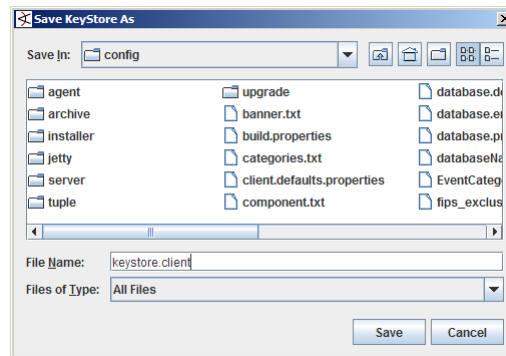
- b Go to **File->New keystore**.



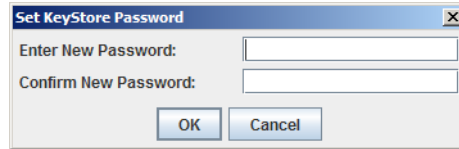
- c Select **JKS** for type of keystore and click **OK**.



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

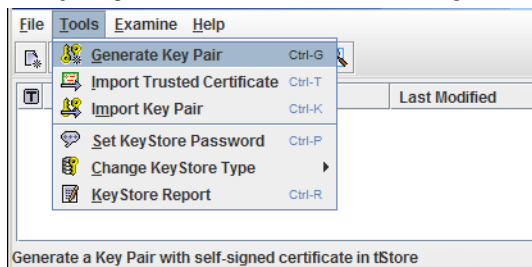


- e Set a password for the keystore and click **OK**.

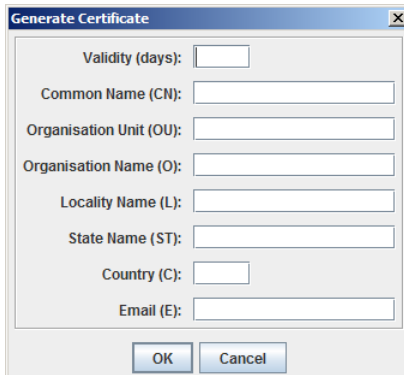


- 2 Create a new key pair in the `config/keystore.client` of the SmartConnector. (If you already have a keypair that you would like to use, you can import the existing key pair into the client's `config/keystore.client`. See section [“Import a Key Pair”](#) on page 54 for details.)

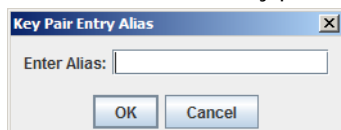
- a In keytoolgui, click **Tools->Generate Key Pair**.



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



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



- d** Set a password for the key pair and click **OK**.
- e** At the successful generation dialog, click **OK**.

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

- 3** Create a client SSL configuration text file in the `user/agent` directory and name it `agent.properties` for a connector. The contents of this file (whether client or agent) should be as follows:

```
auth.null=true
ssl.client.auth=true
cac.login.on=false
ssl.keystore.path=config/keystore.client
ssl.keystore.password=<client.keystore_password>
```



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

Note

- 4** Export the client's (Connector) certificate using `keytoolgui`. See section ["Export a Certificate" on page 54](#) for details.
- 5** Import the CA's certificate of the client's certificate (in case you are using CA-signed certificate) or the client's certificate itself (in case you are using a self-signed certificate) into the Manager's truststore, `/config/jetty/truststore`. see section ["Import a Certificate" on page 55](#) for details.
- 6** Restart the Manager.
- 7** Restart the client (Connector).

Migrating from one certificate type to another

When you migrate from one certificate type to another on the Manager, 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 58](#).
- 2** Follow the instructions in ["Verifying SSL Certificate Use" on page 78](#) 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 SSL Certificate" on page 62](#).
- 2** Follow the instructions in ["Verifying SSL Certificate Use" on page 78](#) 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 SSL Certificate” on page 62](#).
- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 78](#) 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 is the name of the machine on which you created the certificate

Sample output for verifying SSL certificate use

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

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

```
SSL Client
```

```
truststore C:\arcsight\Console\current\jre\lib\security\cacerts
```

```
    Type                                JKS
```

```
    Demo CA trusted                      no
```

```
    Trusted CA                          DigiCert Assured ID Root CA
```

```
[digicertassuredidrootca]
```

```
    Trusted CA                          TC TrustCenter Class 2 CA II
```

```
[trustcenterclass2caii] .
```

```
.
```

```
.
```

```
Demo CA
```

```
    keystore    C:\arcsight\Console\current\config\keystore.tempca
```

```
Exiting...
```

Using Certificates to Authenticate Users to ArcSight

Instead of using a user name and password to authenticate a user to the Manager or ArcSight Web, you can configure these systems to use a digitally-signed user certificate. This section tells you how to do that. This capability is useful 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 are grayed out. Simply select the Manager to which you want to connect and click **OK** to log in.

Using the Certificate Revocation List (CRL)

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

Before you use the CRL feature, make sure:

- Your certificates are issued/signed by a valid Certificate Authority or an authority with an ability to revoke certificates.
- The CA's root certificate is present in the Manager's `<ARCSIGHT_HOME>/config/jetty/truststore` directory.
The Manager validates the authenticity of the client certificate using the root certificate of the signing CA.
- You have a current CRL file provided by your CA.
The CA updates the CRL file periodically as and when additional certificates get invalidated.

To use the CRL feature:

- 1 Make sure you are logged out of the Console.

- 2 Copy the CA-provided CRL file into your Manager's <ARCSIGHT_HOME>/config/jetty/crls directory.

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

Other Tools for Managing Key- and Truststores

keytool

The `keytool` utility is the command-line version of `keytoolgui` that you can use to manipulate the keystores and truststores directly. Use the `keytool` utility on UNIX environments without X11 or whenever a command-line option is more suitable.

Use `keytool -help` for a complete list of all command options and their arguments.

To use `keytool`, enter this command:

```
arcsight keytool [option] -store <store value>
```

where <store value> can be:

- `managerkeys`—Manager keystore
- `managercerts`—Manager truststore
- `webkeys`—Web keystore
- `webcerts`—Web truststore
- `ldapkeys`—Manager LDAP Client keystore
- `ldpcerts`—Manager LDAP Client truststore
- `clientkeys`—Client keystore
- `clientcerts`—Client truststore

On SmartConnector hosts, use:

```
arcsight agent keytool [option] -store <store value>
```

The following is an example for creating a 2048-bit, RSA key-pair with the *mykey* alias that expires in 10 years (3650 days).

```
arcsight keytool -v -genkeypair -alias mykey -validity 3650  
-keyalg rsa -keysize 2048 -store managerkeys
```

The following is an example for exporting the above key-pair as a "self-signed" RFC-1421 compliant ASCII certificate.

```
arcsight keytool -exportcert -alias mykey -v -store managerkeys  
-rfc -file export_mykey.pem
```

You can also SCP your keystore file to a computer where the ArcSight Console is installed and use `keytoolgui` to make changes before uploading back to the remote server.

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
```

Two 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, if applicable:

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


Running the Manager Configuration Wizard

This chapter covers the following topics:

[“Running the Wizard” on page 83](#)

[“Authentication Details” on page 89](#)

You can change some configuration parameters by running the `managersetup` program at any time after you have installed and configured your system.

Running the Wizard

Run the wizard as user *arcsight*. Before you run the `managersetup` wizard, stop your Manager by running the following command:

```
/etc/init.d/arcsight_services stop manager
```

Verify that the Manager has stopped by running the following command (as user *arcsight*):

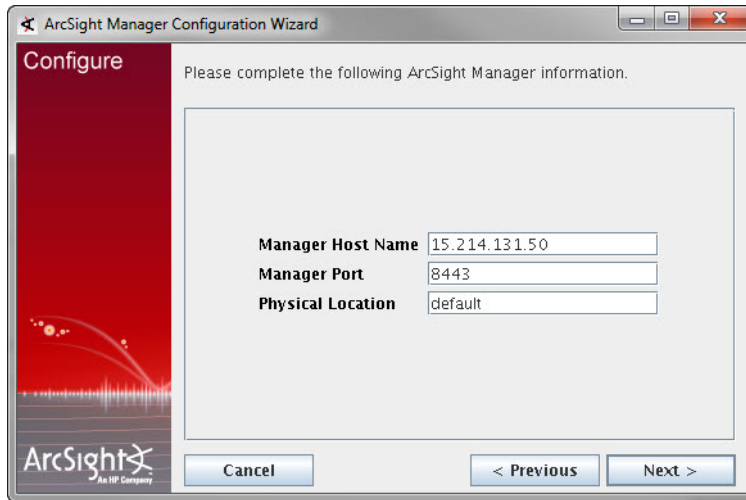
```
/etc/init.d/arcsight_services status all
```

To start the wizard, run the following from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

- 1 To change the hostname or IP address for your Manager host, enter the new one here. The Manager host name that you enter in this dialog appears on the Manager certificate. If you change the host name, be sure to regenerate the Manager's

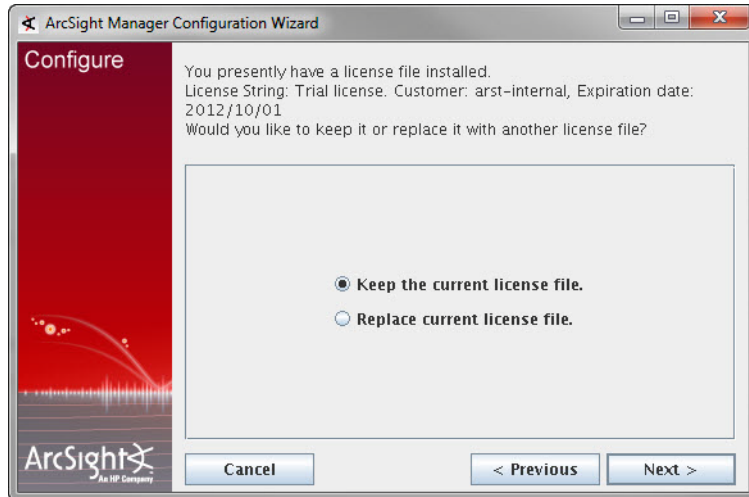
certificate in [Step 4 on page 85](#). We recommend that you do not change the Manager Port number.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background with the text 'Please complete the following ArcSight Manager information.' Below this is a form with three fields: 'Manager Host Name' with the value '15.214.131.50', 'Manager Port' with the value '8443', and 'Physical Location' with the value 'default'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

The managersetup Configuration Wizard establishes parameters required for the Manager to start up when you reboot.

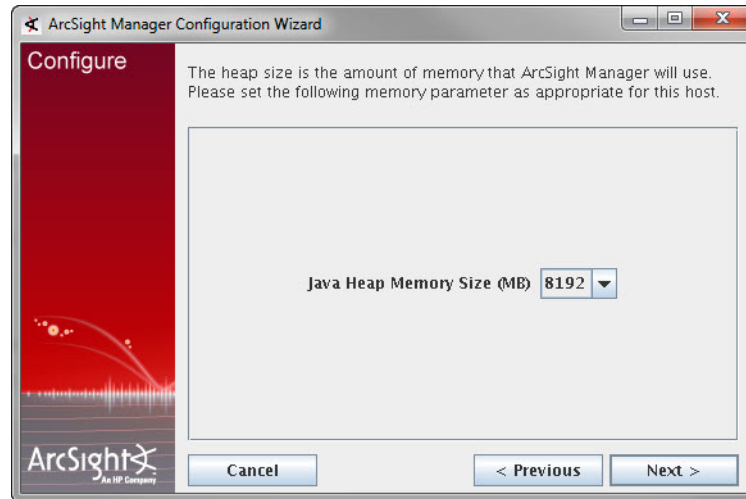
- 2 If you would like to replace your license file with a new one, select **Replace current license file**. otherwise accept the default option of **Keep the current license file**.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard, specifically the license selection screen. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background with the text 'You presently have a license file installed. License String: Trial license. Customer: arst-internal, Expiration date: 2012/10/01. Would you like to keep it or replace it with another license file?'. Below this text are two radio button options: 'Keep the current license file.' (which is selected) and 'Replace current license file.'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

If you selected **Replace the current license file**, you are prompted to either enter its location or navigate to the new license file.

- 3 Select the Java Heap memory size from the dropdown menu.



The Java Heap memory size is the amount of memory that ESM allocates for its heap. (Besides the heap memory, the Manager also uses some additional system memory.)

- 4 The Manager controls SSL certificate type for communications with the Console, so the wizard prompts you to select the type of SSL certificate that the Manager is using. If you changed the Manager host name in [Step 1 on page 83](#), select **Replace with new Self-Signed key pair**, otherwise select **Do not change anything**.



If you selected **Replace with new Self-Signed key pair**, you are prompted to enter the password for the SSL key store and then details about the new SSL certificate to be issued.

- 5 Accept the default in this screen and click **Next**.

ArcSight Manager Configuration Wizard

Configure

Please complete the following information about the database.

Logger JDBC URL

Database Password

Cancel < Previous Next >

- 6 Select the desired authentication method and click **Next**.

ArcSight Manager Configuration Wizard

Configure

Please select a method for authenticating users with ArcSight Manager.

☒ Password Based Authentication

☐ Password Based and SSL Client Based Authentication

☐ Password Based or SSL Client Based Authentication

☐ SSL Client Only Authentication

Cancel < Previous Next >

- 7 Select the method for authenticating the users. See [“Authentication Details”](#) on page 89 for more details on each of these options.

ArcSight Manager Configuration Wizard

Configure

Please select a method for authenticating users with ArcSight Manager.

NOTE: If you are not sure, please select Built-In Authentication.

☒ Built-In Authentication

☐ RADIUS Authentication (SecurID, PremierAccess)

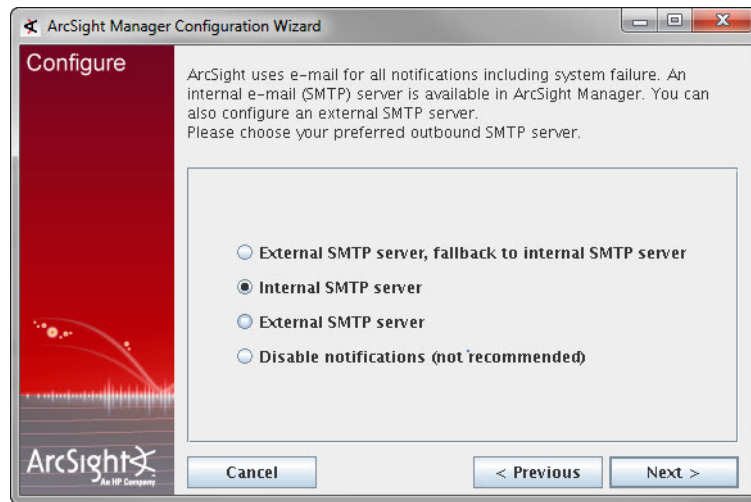
☐ Microsoft Active Directory

☐ Simple LDAP Bind

☐ Custom JAAS Plugin Configuration

Cancel < Previous Next >

- 8 Accept the default and click **Next** or configure a different email server for notification.

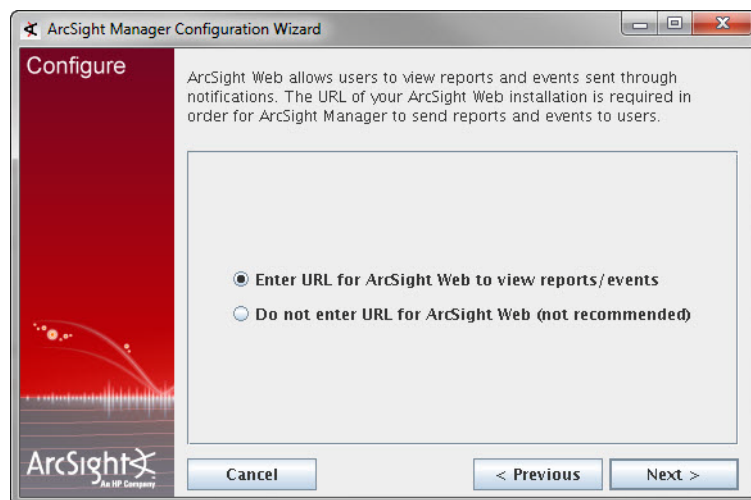


Caution

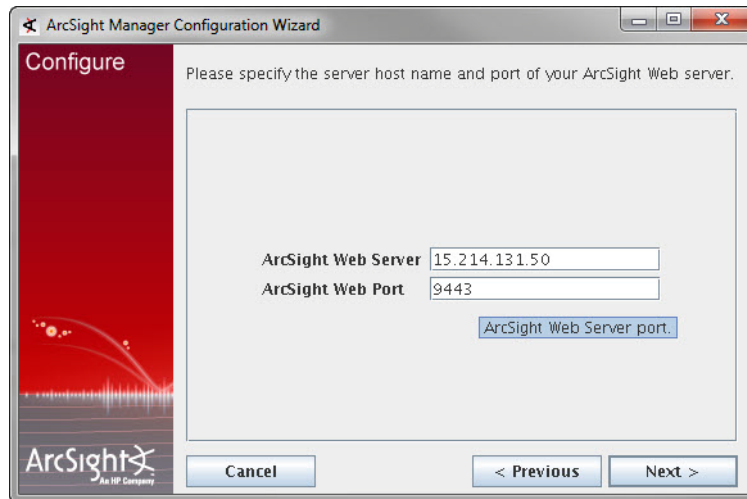
You must set up notification and specify notification recipients in order to receive system warnings. The importance of this step is sometimes overlooked, leading to preventable system failures.

If you choose External SMTP Server, additional screens appear (not shown), to which the following steps apply:

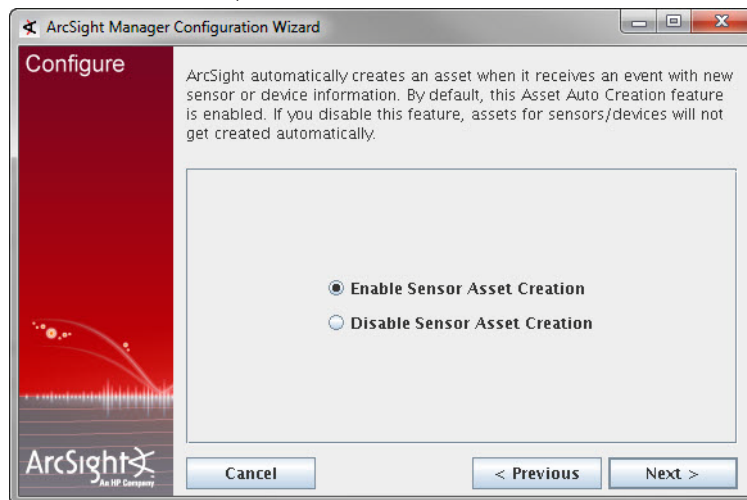
- a Enter the name of the outbound **SMTP Server** to use for notifications.
 - b Enter the **From Address** that the Manager is to place in the From field of outgoing emails.
 - c Enter the **Error Notification Recipients** as a comma-separated list of email addresses to which the Manager should send error notifications.
 - d Select **Use my server for notification acknowledgements**.
 - e Enter the SMTP server and account information. This includes the incoming email server and the server protocol, and the username and password for the email account to be used.
- 9 Select **Do not enter URL for ArcSight Web** and click **Next**.



- 10 Specify the ArcSight Web server and port.



- 11 The Manager can automatically create an asset when it receives an event with a new sensor or device information. By default, assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation**.



- 12 Click **Next** again in the following screen to save your changes.

- 13 Click **Finish** in the final screen.

You have completed the Manager setup program. You can now start the Manager by running the following as user *arcsight*:

```
/etc/init.d/arcsight_services start manager
```


Authentication Details

The authentication options enable you to select the type of authentication to use when logging into the Manager.



Caution

- In order to use PKCS#11 authentication, you must select one of the SSL based authentication methods.
- If you plan to use PKCS #11 token with ArcSight Web, make sure to select **Password Based or SSL Client Based Authentication**.
- PKCS#11 authentication is not supported with Radius, LDAP and Active Directory authentication methods.

See the appendix "Using the PKCS#11 Token," in the ESM Installation and Configuration Guide, for details on using a PKCS #11 token such as the Common Access Card (CAC).

By default, the system uses its own, built-in authentication, but you can specify third party, external authentication mechanisms, such as RADIUS Authentication, Microsoft Active Directory, LDAP, or a custom JAAS plug-in configuration.

How External Authentication Works

The Manager uses the external authentication mechanism for authentication only, and not for authorization or access control. That is, the external authenticator only validates the information that users enter when they connect to the Manager by doing these checks:

- The password entered for a user name is valid.
- If groups are applicable to the mechanism in use, the user name is present in the groups that are allowed to access ArcSight Manager.

Users who pass these checks are authenticated.

Once you select an external authentication mechanism, all user accounts, including the admin account, are authenticated through it.

Guidelines for Setting Up External Authentication

Follow these guidelines when setting up an external authentication mechanism:

- Users connecting to the Manager must exist on the Manager.
- User accounts, including admin, must map to accounts on the external authenticator. If the accounts do not map literally, you must configure internal to external ID mappings in the Manager.
- Users do not need to be configured in groups on the Manager even if they are configured in groups on the external authenticator.
- If user groups are configured on the Manager, they do not need to map to the group structure configured on the external authenticator.
- Information entered to set up external authentication is *not* case sensitive.

- To restrict information users can access, set up Access Control Lists (ACLs) on the Manager.



If you configure the Manager using **Password Based and SSL Client Based Authentication** or **SSL Client Only Authentication**, be aware that ArcSight Web does not support these modes. So:

- If you plan to use ArcSight Web, you will need to configure your Manager to use **Password Based Authentication** or **Password Based or SSL Client Based Authentication** as your authentication method.
- If you plan to use PKCS#11 authentication with ArcSight Web, be sure to select **Password Based or SSL Client Based Authentication** only.

Password Based Authentication

Password-based authentication requires users to enter their User ID and Password when logging in. You can select the built-in authentication or external authentication.

Built-In Authentication

This is the default authentication when you do not specify a third party external authentication method.

If you selected this option, you are done.

Setting up RADIUS Authentication

To configure ArcSight Manager for RADIUS Authentication, choose **RADIUS Authentication** and supply the following parameter values:

Parameter	Description
Authentication Protocol	Which authentication protocol is configured on your RADIUS server: PAP, CHAP, MSCHAP, or MSCHAP2.
RADIUS Server Host	Host name of the RADIUS server. To specify multiple RADIUS servers for failover, enter comma-separated names of those servers in this field. For example, server1, server2, server3. If server1 is unavailable, server2 is contacted, and if server2 is also unavailable, server3 is contacted.
RADIUS Server Type	Type of RADIUS server: <ul style="list-style-type: none"> • RSA Authentication Manager • Generic RADIUS Server • Safeword PremierAccess
RADIUS Server Port	Specify the port on which the RADIUS server is running. The default is 1812.
RADIUS Shared Secret	Specify the RADIUS shared secret string used to verify the authenticity and integrity of the messages exchanged between the Manager and the RADIUS server.

Setting up Active Directory User Authentication

To authenticate users using a Microsoft Active Directory authentication server, choose **Microsoft Active Directory**. Communication with the Active Directory server uses LDAP and optionally SSL.

The next panel prompts you for this information.

Parameter	Description
Active Directory Server	Host name of the Active Directory Server.
Enable SSL	Whether the Active Directory Server is using SSL. The default is True (SSL enabled on the AD server). No further SSL configuration is required for the AD server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the AD server side, not the manager.
Active Directory Port	Specify the port to use for the Active Directory Server. If the AD server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the AD server, use port 389.
Search Base	Search base of the Active Directory domain; for example, DC=company, DC=com.
User DN	Distinguished Name (DN) of an existing, valid user with read access to the Active Directory. For example, CN=John Doe, CN=Users, DC=company, DC=com. The CN of the user is the "Full Name," not the user name.
Password	Domain password of the user specified earlier.
Allowed User Groups	Comma-separated list of Active Directory group names. Only users belonging to the groups listed here will be allowed to log in. You can enter group names with spaces.

Specify any user who exists in AD to test the server connection.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the AD server.

Configuring AD SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store

<ARCSIGHT_HOME>/jre/lib/security/cacerts, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the Administrator's Guide.

Setting up LDAP Authentication

The ArcSight Manager binds with an LDAP server using a simple bind. To authenticate users using an LDAP authentication server, choose **Simple LDAP Bind** and click **Next**. The next panel prompts you for this information.

Parameter	Description
LDAP Server Host	Specify the host name of the LDAP Server.
Enable SSL	Whether the LDAP Server is using SSL. The default is True (SSL enabled on the LDAP server). No further SSL configuration is required for the LDAP server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the LDAP server side, not the manager.
LDAP Server Port	Specify the port to use for the LDAP Server. If the LDAP server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the LDAP server, use port 389.

Specify any user who exists in LDAP to test the server connection.

Enter a valid Distinguished Name (DN) of a user (and that user's password) that exists on the LDAP server; for example, CN=John Doe, OU= Engineering, O=YourCompany. This information is used to establish a connection to the LDAP server to test the validity of the information you entered in the previous panel.



Note

LDAP groups are not supported. Therefore, you cannot allow or restrict logging into the Manager based on LDAP groups.

If you configure your Manager to use LDAP authentication, ensure that you create users on the Manager with their Distinguished Name (DN) information in the external ID field. For example, CN=John Doe, OU= Engineering, O=YourCompany.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the LDAP server.

Configuring LDAP SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store

<ARCSIGHT_HOME>/jre/lib/security/cacerts, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the Administrator's Guide.

Using a Custom Authentication Scheme

From the Manager Setup Wizard, you can choose the **Custom JAAS Plug-in**

Configuration option if you want to use an authentication scheme that you have built. (Custom Authentication is not supported from the ArcSight Command Center.) You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.

Password Based and SSL Client Based Authentication

Your authentication will be based both upon the username and password combination as well as the authentication of the client certificate by the Manager.



Using PKCS#11 provider as your SSL Client Based authentication method within this option is not currently supported.

Password Based or SSL Client Based Authentication

You can either use the username/password combination or the authentication of the client certificate by the Manager (for example PKCS#11 token) to login if you select this option.

SSL Client Only Authentication

You will have to manually set up the authentication of the client certificate by the Manager. See the Administrator's Guide for details on how to do this.

You can either use a PKCS#11 Token or a client keystore to authenticate.

Chapter 5

Managing Resources

Some administrator tasks necessary to manage ESM are performed in the Command Center or the ArcSight Console. The details for performing such tasks are documented in the ArcSight Command Center User's Guide or the ArcSight Console User's Guide. This chapter points you to the location where these tasks are documented.

This chapter in the ArcSight Console User's Guide....	...discusses these topics
Chapter 20, Managing Users and Permissions, on page 595	<ul style="list-style-type: none">• "Managing Users" on page 595• "Managing Permissions and Resources" on page 601• "Managing Notifications" on page 613
Chapter 23, Modeling the Network, on page 693	<ul style="list-style-type: none">• "Modeling the Network" on page 693• "Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories" on page 715• "Managing Customers" on page 728
Chapter 7, Filtering Events, on page 175	<ul style="list-style-type: none">• "Creating Filters" on page 175• "Moving or Copying Filters" on page 178• "Deleting Filters" on page 179• "Debugging Filters to Match Events" on page 179• "Applying Filters" on page 181• "Importing and Exporting filters" on page 182• "Using Filter Groups" on page 182• "Investigating Views" on page 183• "Modifying Views" on page 187

This chapter in the ArcSight**Console User's Guide....****...discusses these topics**

Chapter 21, Managing Resources, on page 621

- "Managing File Resources" on page 621
- "Locking and Unlocking Resources" on page 625
- "Selecting Resources" on page 626
- "Finding Resources" on page 627
- "Visualizing Resources" on page 630
- "Viewing Resources in Grids" on page 633
- "Validating Resources" on page 633
- "Extending Audit Event Logging" on page 639
- "Saving Copies of Read-Only Resources" on page 640
- "Common Resource Attribute Fields" on page 640
- "Managing Packages" on page 642

Chapter 22, Managing SmartConnectors, on page 655

- "Selecting and Setting SmartConnector Parameters" on page 655
 - "Managing SmartConnector Filter Conditions" on page 673
 - "Setting Special Severity Levels" on page 674
 - "Sending Model Mappings to SmartConnectors" on page 676
 - "Sending Control Commands to SmartConnectors" on page 676
 - "Managing SmartConnector Groups" on page 683
 - "Managing SmartConnector Resources" on page 684
 - "Importing and Exporting SmartConnector Configurations" on page 685
 - "Upgrading SmartConnectors" on page 687
-

Appendix A

Administrative Commands

This appendix provides information about assorted Administrative commands.

[“ArcSight_Services Command” on page 97](#)
[“ArcSight Command Index” on page 98](#)
[“ESM ArcSight Commands” on page 98](#)
[“CORR-Engine ArcSight Commands” on page 134](#)

ArcSight_Services Command

The `arcsight_services` command syntax and options are described below:

Description	A tool for managing component services. For all components except connectors run this as user <i>arcsight</i> . For connectors, run it as <i>root</i> .	
Applies to	All components	
Syntax	<code>/etc/init.d/arcsight_services <action> <component></code>	
Service Actions	<code>start</code>	Start the specified component, and any components it depends on. To start the connector service, run it as user <i>root</i> .
	<code>stop</code>	Stop the specified component and any components that depend on it. To stop the connector service, run it as user <i>root</i> .
	<code>restart</code>	Complete a controlled stop and restart of the specified component service and any component it depends on. To restart the connector service, run it as user <i>root</i> . Do not use stop, then start, to restart a service.
	<code>status</code>	This provides the component version and build numbers followed by whether each service is available.
	<code>help</code>	Provides command usage (no component)
	<code>Version</code>	Print the complete version numbers of all components

	all	This is the default if no component is specified. To apply to connectors run it as user <i>root</i> , which works for all components.
Component Services	arcsight_web	The ArcSight Web service
	manager	The ESM Manager
	logger_httpd	The Logger Apache httpd service
	logger_servers	The Logger service
	logger_web	The Logger Web service
	mysqld	The MySQL database
Examples	/etc/init.d/arcsight_services start	
	/etc/init.d/arcsight_services stop manager	
	/etc/init.d/arcsight_services status all	
	/etc/init.d/arcsight_services stop	

ArcSight Command Index

This list includes both the ESM *arcsight* commands and the CORR-Engine *arcsight* Commands.

Alphabetical ArcSight Commands List

ACLReportGen	exceptions	reenableuser
agent logfu	export_system_tables	refcheck
agent tempca	exportdatausage	regex
agentcommand	flexagentwizard	replayfilegen
agents	groupconflictingassets	resetpwd
agentsvc	idensesetup	resvalidate
agenttempca	import_system_tables	ruledesc
agentup	keytool	runcertutil
arcdt	keytoolgui	runmodutil
archive	kickbleep	runpk12util
archivefilter	listsubjectdns	script
bleep	logfu	searchindex
bleepsetup	managerinventory	sendlogs
changepassword	manager-reload-config	tee
checklist	managersetup	tempca
configbackup	managereadddump	threaddumps
console	managerup	tproc
consolesetup	monitor	webserversetup
disasterrecovery	netio	websetup
downloadcertificate	package	whois
	portinfo	

ESM ArcSight Commands

To run an ArcSight command script on a component, open a command window and switch to the <ARCSIGHT_HOME> directory. The *arcsight* commands run using the file *arcsight.sh* in <ARCSIGHT_HOME>\bin. The general syntax is as follows:

```
bin\arcsight <command_name> [parameters]
```

In general, commands that accept a path, accept either a path that is absolute or relative to <ARCSIGHT_HOME>. Running the command from <ARCSIGHT_HOME> and prefixing it with `bin\` enables you to use the shell's capabilities in looking for relative paths.

Not all parameters are required. For example, username and password may be a parameter for certain commands, such as the Manager and Package commands, but the username and password are only required if the command is being run from a host that does not also host the Manager.

ACLReportGen

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

agent logfu

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

agent tempca

Description	Inspect and manage temporary certificates for a SmartConnector host machine
Applies to	SmartConnectors
Syntax	<code>agent tempca</code>
Parameters	For Parameters, see <code>tempca</code> command (Manager)
Examples	To run: <code>arcsight agent tempca</code>

agentcommand

Description	Send a command to SmartConnectors
Applies to	SmartConnectors
Syntax	<code>agentcommand -c (restart status terminate)</code>
Parameters	<code>-c</code> Command: restart, status, or terminate
Examples	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

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

agentsvc

Description	Install ArcSight SmartConnector as a service.	
Applies to	SmartConnectors	
Syntax	<code>agentsvc -i -u <user></code>	
Parameters	<code>-i</code>	Install the service
	<code>-u <user></code>	Run service as specified user
Examples	To install a SmartConnector as a service: <code>arcsight agentsvc</code>	

agenttempca

Description	See the agent tempca command	
Applies to	SmartConnectors	

agentup

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

arcdt

Description	A utility that enables you run diagnostic utilities such as session wait times, and thread dumps about your system, which helps Customer Support analyze performance issues on your components	
Applies to	Manager	
Syntax	<code>arcdt diagnostic_utility utility_Parameters</code>	

diagnostic_utility	<p>Utilities you can run are:</p> <p>runsql—Run SQL commands contained in a file that is specified as a parameter of this utility.</p> <p>Required Parameter:</p> <p>-f <sqlfile> —The file containing the sql statements to be executed.</p> <p>Optional Parameters:</p> <p>-fmt <format> —The format the output should be displayed in (where relevant), choices are: html/text (text)</p> <p>-o <outputfile> —File name to save output to. ()</p> <p>-rc <row_count> —The number of rows to be shown as a result of a select. (10000)</p>
Parameters	<p>-se <sessionEnd>— if type is EndTime or mrt, value is like yyyy-MM-dd-HH-mm-ss-SSS-zzz; if type is EventId, value is a positive integer indicating the end of eventId. (2011-06-30-01-00-00-000-GMT)</p> <p>-sr <start_row> —The row number from which you want data to be shown (0)</p> <p>-ss <sessionStart> —if type is EndTime or mrt, value is like yyyy-MM-dd-HH-mm-ss-SSS-zzz; if type is EventId, value is a positive integer indicating the end of eventId. (2011-06-30-00-00-00-000-GMT)</p> <p>-t <terminator> —The character that separates SQL statements in the input file. (.)</p> <p>-type <type> —Session type for sql query: EndTime, mrt, or EventId (EndTime)</p> <p>-cmt — Flag indicating whether all inserts and updates should be committed before exiting.</p> <p>-sp — Flag specifying whether output should be saved to disk or not.</p> <p>session-waits—Retrieve the currently running JDBC (Java Database Connection) sessions and their wait times.</p> <p>Required Parameter:</p> <p>-sp — Flag specifying whether output should be saved to disk or not.</p> <p>Optional Parameters:</p> <p>-c <count> — The number of times we want to query the various session tables. (5)</p> <p>-f <frequency> — The time interval (in seconds) between queries to the session tables. (20)</p>
	<p>-fmt <format> — The format the output should be displayed in (where relevant), choices are: html/text (text)</p> <p>-o <outputfile> — File name to save output to. ()</p>

	thread-dumps—Obtain thread dumps from the Manager. Optional parameters which can be specified
	-c <count> The number of thread dumps to request. (3)
	-f <frequency> The interval in SECONDS between each thread dump request. (10)
	-od <outputdir> The output directory into which the requested thread dumps have to be placed. ()
help	Use these help Parameters (no dash) to see the Parameters, a list of commands, or help for a specific command.
help commands	
help <command>	
Examples	To find out the number of cases in your database:
	1 Create a file called <code>sample.txt</code> in <code><ARCSIGHT_HOME>/temp</code> on the Manager with this SQL command:
	<code>select count(*) from arc_resource where resource_type=7;</code>
	2 Run this command in <code><ARCSIGHT_HOME>/bin</code> :
	<code>arcsight arcdt runsql -f temp/sample.txt</code>

If not done correctly, you might get no result querying the `ArcSight.events` table from `arcdt`. For example, to run SQL to query events for a specific time period, follow the steps below:

- 1 Create a file such as `1.sql` in `/tmp/` containing this SQL:

```
"select * from arcsight.events where arc_deviceHostName =
'host_name' limit 2;"
```

- 2 Run `arcdt` and pass the created SQL file as parameter, and also specify the time period to examine.

```
./arcsight arcdt runsql -f /tmp/1.sql -type EndTime -ss <start
time> -se <end time>
```

Obviously, the result will be empty if there are no events in the specified time period.

archive

	Import or export resources (users, rules, and so on) to or from one or more XML files.	
Description	Note: Generally, there is no need to use this command. The Packages feature in the ArcSight Console is more robust and easier to use for managing resources.	
Applies to	Manager, Console	
Syntax	<code>archive -f <archivefile> [Parameters]</code>	
Required Parameter	<code>-f <archivefile></code>	The input (import) or the output (export) file specification. Note: Filename paths can be absolute or relative. Relative paths are relative to <code><ARCSIGHT_HOME></code> , not the current directory.

Optional Parameters	<code>-action <action></code>	Possible actions include: diff, export, i18nsync, import, list, merge, sort, and upgrade. Default: export.
	<code>-all</code>	Export all resources in the system (not including events).
	<code>-autorepair</code>	Check ARL for expressions that operate directly on resource URI's.
	<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: config/server.defaults.properties
	<code>-conflict <conflictpolicy></code>	The policy to use for conflicts resolution. Possible policies are: default: Prompts user to resolve import conflicts. force: Conflicts are resolved by the new overwriting the old. overwrite: Merges resources, but does not perform any union of relationships. preferpackage: if there is a conflict, it prefers the information in the package that is coming in over what is already there. skip: Do not import resources with conflicts.
	<code>-exportaction <exportaction></code>	The action to assign to each resource object exported. Export actions are: insert: Insert the new resource if it doesn't exist (this is the default). update: Update a resource if it exists. remove: Remove a resource if it exists.
	<code>-format <fmt></code>	Specifies the format of the archive. If you specify nothing, the default is default. default: Prompts user to resolve import conflicts. preferarchive: if there is a conflict, it prefers the information that is coming in over what is there. install: Use this for the first time. update: Merges the archive with the existing content. overwrite: Overwrites any existing content.
	<code>-h</code>	Get help for this command.
	<code>-i</code>	(Synonym for <code>-action import</code> .)
	<code>-m <manager></code>	The Manager to communicate with.

<code>-newids</code>	All archival objects within an archive are given new IDs. All refs to these archival objects are 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>-p <password></code>	Password with which to log in to the Manager.
<code>-param <archiveparamsfile></code>	The source file for parameters used for archiving. Any parameters in the named file 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 <hostname> -pkcs11 -f <file path></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. This is used for all commands that use the <code>-f</code> to specify an output file and use a separate file as the input.
<code>-standalone</code>	Operate directly on the Database, not the Manager. Warning: 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
<code>-uri <includeURIs></code>	The URIs 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 <includeURIchildren></code>	The URIs to export (there is no effect during import). All child resources of the specified resources are exported. A parent of a specified resource is only exported if the specified resource is dependent on it.
<code>-xrefids</code>	Exclude reference IDs. This option determines whether to include reference IDs during export. This is intended only to keep changes to a minimum between exports. Do not use this option without a complete understanding of its implications.

<code>-xtype <excludeTypes></code>	The types to exclude during export. No effect during import. Exclude types must be valid type names, such as Group, Asset, or ActiveChannel.
<code>-xtyperef <excludeTypeRefs></code>	The types to exclude during export (there is no effect during import). This is the same as <code>-xtype</code> , except it also excludes all references of the given type. These must include only valid type names such as Group, Asset, and ActiveChannel.
<code>-xuri <excludeURIs></code>	The URIs to exclude during export. No effect during import. Resources for which all possible URIs are explicitly excluded are not exported. Resources which can still be reached by a URI that is not excluded are still exported.
<code>-xurichildren <excludeURIchildren></code>	The URIs to exclude during export (there is no effect during import). These exclusions are such that all URIs for the children objects must be included in the set before the object will be excluded. In other words, they can still be exported if they can be reached through any path that is not excluded.

Examples

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:

```
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"
```

Archive Command Details



Note

Ordinarily, you should use the packages feature to archive and import resources. For more information about packages and how to use them, see the "Managing Packages" topic in ArcSight Console Online Help. Also, see the packages command.

You can use the `archive` command line tool to import and export resources. It is useful for managing configuration information, for example, importing asset information collected from throughout your enterprise. You can also use this tool to archive resources so you can restore it after installing new versions of this system.

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 the system. Generally it is easier to use packages.

This command displays a resource in the archive menu list of resources only if the user running the utility has top-level access to the resource. Access is different for each mode.

Remote Mode

In remote mode, you can import or export from either a Manager or ArcSight Console installation and can perform archive operations while the Manager is running.

```
arcsight archive -u Username -m Manager [-p Password] -f Filename
                    [-i | -sort] [-q] ...
```



Caution

The cacerts file on the Manager host must trust the Manager's certificate. You may have to update cacerts if you are using demo certificates by running:

```
arcsight tempca -ac
```

You do not need to run the above command if you run the `archive` command from the Console.

When you run the archive utility in the remote mode, it runs as the user specified in the command line. However, even users with the highest privilege level (administrator) do not have top level access to, for example, the user resource (All Users). Thus, the User resource does not show up in the list of resources. You can export users with the `-uri` option, but if you want to use the `-u` option, use the Standalone mode.

To export user resources, you can use the `-uri` option and specify a user resource to which you have direct access. For example:

```
arcsight archive -u <username> -m <manager_hostname> -format
exportuser -f exportusers.xml -uri "/All Users/Administrators/John
```

Standalone Mode

In standalone mode, from the computer where the Manager is installed, you can connect directly to the database to import or export resource information, however, the Manager must be shut down before you perform archive operations.



Caution

Do not run the archive tool in standalone mode against a database currently in use by a Manager as it is possible to corrupt the database.

When you run the archive utility in standalone mode, it runs as Root user. This is a special system user which has top level access to all resources including the User resource (which is All Users), so, for example, User Resource shows up in the list of resources.

The basic syntax for the `archive` command in standalone mode is the following:

```
arcsight archive -standalone -f Filename [-i | -sort] [-q] ...
```



Both remote and standalone archive commands support the same optional arguments.

Note that the standalone mode only works from the archive command found in the Manager installation, and does not work remotely. For example:

```
arcsight archive -standalone -format exportuser -f exportusers.xml
```

Exporting Resources to an Archive

- 1 Make sure the archive tool client can trust the Manager's SSL certificate. Refer to [Chapter 3, SSL Authentication, on page 47](#) for information on managing certificates.

From the <ARCSIGHT_HOME>/bin directory, you can enter the command, `arcsight archive -h` to get help.

- 2 From the <ARCSIGHT_HOME>/bin directory, enter the `arcsight archive` command along with any parameters you want to specify.

This command logs into the Manager then displays a list of Resources available for archiving.



If the Manager is running, you must specify archive commands in remote mode, entering your user name, password, and Manager name to connect to the 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 displays a list of options that let you choose which resource or group 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, you are returned to the command prompt.

Importing Resources from an Archive

- 1 Make sure the archive tool client can trust the Manager's SSL certificate. Refer to [Chapter 3, SSL Authentication, on page 47](#), for information on managing certificates.

- 2 From the <ARCSIGHT_HOME>/bin directory, type `arcsight archive` with its parameters and attach `-i` for import.



Note

If the Manager is running, you must specify archive commands in remote mode, entering your user name, password, and Manager name to connect to the Manager. To run the archive command in standalone mode, accessing resources directly from the 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.

Syntax for Performing Common Archive Tasks

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 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 Manager and use a series of text menus to pick which Resources are 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"
```



Note

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.

archivefilter

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

Examples

To include any resources, for example all Active Channels, whose attributes contain the URI specified by the `-relateduri` option:

```
arcsight archivefilter -source allchannels.xml -f t0.xml -
relateduri "/All Active Channels/ArcSight
Administration/"
```

To include any resources whose parent URI matches the URI specified by the `-uri` option:

```
arcsight archivefilter -source allchannels.xml -f t0.xml -
uri "/All Active Channels/ArcSight Administration/*."
```

To exclude resources whose parent URI matches the URI specified by the `-xuri` option:

```
arcsight archivefilter -source allchannels.xml -f t0.xml -
xuri "/All Active Channels/*."
```

To include all the resources that contain either URIs specified by the two `-relateduri` Parameters:

```
arcsight archivefilter -source allchannelsFilter.xml -f
t0.xml -relateduri "/All Active Channels/ArcSight
Administration/" -relateduri ".*Monitor.*"
```

bleep**Description**

Unsupported stress test command to supply a Manager with security events from replay files (see `replayfilegen`). 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 `arcsight tempca -ac` on the bleep host if the Manager under test is using a demo certificate.

Create the file `config/bleep.properties` using the descriptions in `bleep.defaults.properties`.

Applies to

Manager

Syntax

```
bleep [-c <file>] [-D <key>=<value> [<key>=<value>...]]
```

Parameters

<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

Examples	To run: <code>arcsight bleep</code>
-----------------	--

bleepsetup

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

changepassword

Description	Command to change obfuscated passwords in properties files. The utility prompts for the new password at the command line	
Applies to	Manager	
Syntax	<code>changepassword -f <file> -p <property_name></code>	
Parameters	<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>
Examples	To run: <code>arcsight changepassword</code>	

checklist

Description	ArcSight Environment Check. Used internally by the installer to see if you have the correct JRE and supported OS. This can run from the Connector or Manager.
--------------------	--

console

Description	Run the ArcSight Console
Applies to	Console

Syntax	console [-i] [parameters]	
Parameters	-ast <file>	
	-debug	
	-i	
	-imageeditor	
	-laf <style>	Look and feel style: metal, plastic, plastic3d. The default style for Windows is different than these and not specified. For Unix it is Plastic3d.
	-p <password>	Password
	-port	Port to connect to Manager (default: 8443)
	-redirect	
	-relogin	
	-server	Manager host name
	-slideshow	
	-theme	
	-timezone <tz>	Timezone: such as "GMT" or "GMT-8:00"
	-trace	Log all Manager calls
	-u <name>	User name
Examples	To run the console: ArcSight Console	

consolesetup

Description	Run the ArcSight Console Configuration Wizard to reconfigure an existing installation	
Applies to	Console	
Syntax	consolesetup [-i <mode>] [-f <file>] [-g]	
Parameters	-i <mode>	Mode: console, silent, recorderui, swing
	-f <file>	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode

Examples	To change some console configuration parameters:	
	ArcSight ConsoleSetup	

downloadcertificate

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

exceptions

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

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

export_system_tables

Description	Command 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_dump_system_tables.sql</code> , which is placed in <code>/opt/arcsight/manager/tmp</code> .	
Applies to	Manager	
Syntax	<code>export_system_tables <username> <password> <DBname></code>	
Parameters	<code><username></code>	CORR-Engine username
	<code><password></code>	Password for the CORR-Engine user
	<code><DBname></code>	Name of the Mysql database from which you are exporting the system tables
	<code>-s</code>	include session list tables
Examples	To run: <pre>arcsight export_system_tables <DB username> <password> <DBname></pre> Trend resources are exported, but not trend data from running them. After you import, re-run the trends to generate new data.	

flexagentwizard

Description	Wizard-like command to generate simple ArcSight FlexConnectors
Applies to	SmartConnectors
Syntax	<code>flexagentwizard</code>
Parameters	None
Examples	To run: <pre>arcsight flexagentwizard</pre>

groupconflictingassets

Description	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	
Applies to	Manager	
Syntax	groupconflictingassets	
Parameters	-c	Clean (delete the contents of) the group to receive links to assets before starting. (Default: false)
	-m <host>	Manager host name or address
	-o <name>	Name for group to receive links to assets which have conflicting attributes. (Default: "CONFLICTING ASSETS")
	-p <password>	Password
	-port <n>	Port to connect to Manager (Default: 8443)
	-prot <string>	Protocol { http https } (Default: https)
	-u <name>	User name
	-h	Help
Examples	To run: arcsight groupconflictingassets	

idefensesetup

Description	Wizard to configure iDefense appliance information on the Manager	
Applies to	Manager	
Syntax	idefensesetup	
Parameters	-f <logfilename>	Optional properties file name (silent mode)
	-i <mode>	Mode: swing, Console, recorderui, or silent
	-g	Generate sample properties file for silent mode
	-h	Help
Examples	To launch the iDefense Setup wizard: arcsight idefensesetup	

import_system_tables

Description	Command to import database tables. The file you import from must be the one that export_system_tables utility created. This utility looks for the dump file you specify in /opt/arcsight/manager/tmp/.	
Applies to	Manager	
Syntax	import_system_tables <arcsight_user> <password> <DBname> <dump_file_name>	
Parameters	<arcsight_user>	The database username, as set when you ran the first-boot wizard.
	<password>	Password for the database, as set when you ran the first-boot wizard.
	<DBname>	This is the name of the MySQL database and it is always arcsight.
	<dump_file_name>	Use arcsight_dump_system_tables.sql, which is the name the system gave this dump file when you exported it. If you specify no path, the file is located in /opt/arcsight/manager/tmp/. To specify a different path, use an absolute path. Do not specify a relative path.
Examples	arcsight import_system_tables dbuser mxyzptlk arcsight arcsight_dump_system_tables.sql	
	import_system_tables dbuser mxyzptlk arcsight /home/root/arcsight_dump_system_tables.sql	
	Note: Trend resources are exported, but not trend data from running them. After you import, re-run the trends to generate new data.	

keytool

Description	Runs Java Runtime Environment keytool utility to manage key stores	
Applies to	Manager, Console, SmartConnectors	
Syntax	keytool -store <name>	
Parameters	-store <name>	(Required) Specific store {managerkeys managercerts clientkeys clientcerts ldapkeys ldapcerts webkeys webcerts } (original parameters) All parameters supported by the JRE keytool utility are passed along. Use arcsight keytool
	-help	For a list of parameters and arguments. Also, use the command keytool without arguments or the arcsight prefix for more-detailed help.
Examples	To view Console key store: arcsight keytool -store clientkeys	

keytoolgui

Description	Graphical user interface command for manipulating key stores and certificates
Applies to	Manager, Console
Syntax	keytoolgui
Parameters	None
Examples	To run: arcsight keytoolgui

kickbleep

Description	Runs a simple, standardized test using the bleep utility						
Applies to	Manager						
Syntax	kickbleep						
Parameters	<table><tr><td>-f</td><td>Properties file (silent mode)</td></tr><tr><td>-g</td><td>Generate sample properties file</td></tr><tr><td>-i</td><td>Mode: {swing, console, recorderui, silent} Default: swing</td></tr></table>	-f	Properties file (silent mode)	-g	Generate sample properties file	-i	Mode: {swing, console, recorderui, silent} Default: swing
-f	Properties file (silent mode)						
-g	Generate sample properties file						
-i	Mode: {swing, console, recorderui, silent} Default: swing						
Examples	To run: arcsight kickbleep						

listsubjectdns

Description	Display subject distinguished names (DN) from a key store		
Applies to	Manager, SmartConnectors		
Syntax	listsubjectdns		
Parameters	<table><tr><td>-store name</td><td>Specific store { managerkeys managercerts clientkeys clientcerts ldapkeys ldapcerts } (Default: clientkeys.)</td></tr></table>	-store name	Specific store { managerkeys managercerts clientkeys clientcerts ldapkeys ldapcerts } (Default: clientkeys.)
-store name	Specific store { managerkeys managercerts clientkeys clientcerts ldapkeys ldapcerts } (Default: clientkeys.)		
Examples	To list Distinguished Names in the Console key store: arcsight listsubjectdns		

logfu

Description	Graphical tool for analyzing log files.
Applies to	Manager (See also agent logfu.)

Syntax	logfu {-a -m} [parameters]	
Parameters	-a	Analyze SmartConnector logs
	-f <timestamp>	From time
	-i	Display information about the log files to be analyzed
	-l <timespec>	Analyze only the specified time (Format: <time>{smhd}) Examples: 1d = one day, 4h = four hours
	-m	Analyze Manager logs
	-mempercent <n>	Percent of memory messages to consider for plotting. (Default: 100)
	-noex	Skip exception processing
	-noplot	Skip the plotting
	-t <timestamp>	To time
Examples	To analyze Manager logs for the last 12 hours: arcsight logfu -m -l 12h	

managerinventory

Description	Display configuration information about the installed Manager	
Applies to	Manager	
Syntax	managerinventory	
Parameters	-a <filter>	Attribute filter. Default: "*"
	-f <filter>	Object filter. Default: "Arcsight: *"
	-m <host>	Manager host name or address
	-o <op>	Operation {list, show}. Default is list
	-out <file>	Output filename. Default is stdout
	-p <password>	Password
	-port <n>	Port to connect to Manager (Default: 8443)
	-prot <string>	Protocol { http https } (Default: https)
	-u <name>	User name
	-append	Append to the output file rather than create a new one and overwrite any existing one
	-sanitize	Sanitize the IP addresses and host names

	-h	Get help for this command
Examples	To run: <code>arcsight managerinventory</code>	

manager-reload-config

Description	Load the <code>server.defaults.properties</code> and <code>server.properties</code> files on the Manager	
Applies to	Manager	
Syntax	<code>arcsight manager-reload-config</code>	
Parameters	-diff	Displays the difference between the properties the Manager is currently using and the properties that this command loads
	-as	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
	-t <seconds>	Number of seconds after which the <code>manager-reload-config</code> command stops trying to load the updated properties file on the Manager
Examples	To reload config: <code>arcsight manager-reload-config</code> To view the differences between the properties the Manager is currently using and the properties that this command loads: <code>arcsight manager-reload-config -diff</code>	

managersetup

Description	Run the Manager Configuration Wizard	
Applies to	Manager	
Syntax	<code>managersetup -i console</code>	
Parameters	-i <mode>	Mode: console, silent, recorderui, swing
	-f <file>	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
Examples	To run: <code>arcsight managersetup</code>	

For more information about this command, see [Chapter 4, Running the Manager Configuration Wizard, on page 83](#).

managerthreaddump

Description	Script to dump the Manager's current threads. The threads go into <code>manager/logs/default/server.std.log</code> . Do not inadvertently add a space between <code>manager</code> and <code>threaddump</code> , doing so causes the Manager to restart. Specify this file when running <code>threaddumps</code> , which provides a convenient HTML file with links to all the thread dumps in a summary format.
Applies to	Manager
Syntax	<code>managerthreaddump</code>
Parameters	None
Examples	To run: <code>arcsight managerthreaddump</code>

managerup

Description	Get the current state of the Manager. Returns 0 if the Manager is running and reachable. Returns 1 if it is not.
Applies to	Manager
Syntax	<code>managerup</code>
Parameters	None
Examples	To check that the Manager is up, running, and accessible: <code>arcsight managerup</code>

monitor

Description	Tool used in conjunction with Network Management Systems	
Applies to	Manager	
Syntax	<code>monitor</code>	
Parameters	<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

	-sanitize	Sanitize IP address and host names (Default: false)
	-u <name>	User name
Examples	To run: arcsight monitor	

netio

Description	Primitive network throughput measurement utility	
Applies to	Manager	
Syntax	netio	
Parameters	-c	Client mode (Default: false)
	-n <host>	Host to connect to (Client mode only)
	-p <port>	Port (Default: 9999)
	-s	Server mode
Examples	To run: arcsight netio	

package

Description	Import or export resources (users, rules, and so on) to or from one or more XML files (.arb files).	
	Use this command instead of the archive command. Note: Some functionality for this command are available from the GUI only.	
Applies to	Manager, Database, Console	
Syntax	package -action <action-to-be-taken> -package <package URI> -f <package-file>	
Parameters	- action <action>	Creates a new package based upon one or more packages that you specify. The possible actions include bundle, convertarchives, export, import, install, uninstall. The default is export
	-config <file>	The primary configuration file to use. Default is config/server.defaults.properties
	-convertbaseuri <baseuri>	The base URI for packages that are converted from archives. This option is only used in conjunction with the -action convertarchives option

-f <path>	The location of the package .arb bundle file. File name paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME>
-m <manager>	The Manager to communicate with
-p <password>	The password with which to log in to the Manager. A password is not needed and not used in standalone mode, because the connection is made using the stored database account. Password is required otherwise.
-package <packagerefs>	The URI(s) of the package(s). This option is used in conjunction with -action install and -action uninstall in order to list which packages to operate upon
-pc <privateConfig>	This configuration file overrides the server.defaults.properties file. The default location is config/server.properties
-pkcs11	Use this option when authenticating with a PKCS#11 provider. For example, arcsight package -m <hostname> -pkcs11 -f <file path>
-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 -f command which specifies an output file
-u <username>	The user name used for logging in to the Manager
-standalone	Operate directly on the Database not the Manager

Examples	To convert a previously archived package:
	<pre>arcsight package -action convertarchives -convertbaseuri "/All Packages/Personal/Mypackage" -source sourcefile.xml -f packagebundle.arb</pre>
	To install a package:
	<pre>arcsight package -action install -package "/All Packages/Personal/Mypackage" -u username -p password -m managename</pre>
	To uninstall a package:
	<pre>arcsight package -action uninstall -package "/All Packages/Personal/Mypackage" -standalone -config /config/server.defaults.properties -pc /config/server.properties</pre>
	To import a package through the Manager:
	<pre>arcsight package -action import -f packagebundle.arb -u username -p password -m managename</pre>
	To export a package:
	<pre>arcsight package -action export -package "/All Packages/Personal/Mypackage" -f packagebundle.arb -u username -p password -m managename</pre>
	To export multiple packages:
	<pre>arcsight package -action export -package "/All Packages/Personal/PackageOne" -package "/All Packages/Personal/PackageTwo" -f packagebundle.arb -u username -p password -m managename</pre>
	To export packages in a standalone mode (directly from the database) Make sure that the Manager is not running:
	<pre>arcsight package -action export -package "/All Packages/Personal/Mypackage" -f packagebundle.arb -u username -p password -standalone -config server.default.properties -pc server.properties</pre>
	To combine xml files from multiple packages into one package:
	<pre>arcsight package -action bundle -f myPkgNew.arb -source chnpkg.xml -source filterpkg.xml -source rulepkg.xml</pre>
	In the above example, chnpkg.xml, filterpkg.xml, and rulepkg.xml files are extracted from their respective packages and are bundled in one package bundle called myPkgNew.arb.

portinfo

Description	Script used by the portinfo tool of the Console. Displays common port usage information for a given port	
Applies to	Console	
Syntax	portinfo port	
Parameters	port	Port number
Examples	To run: arcsight portinfo	

reenableuser

Description	Re-enable a disabled user account
Applies to	Manager
Syntax	<code>reenableuser <username></code>
Parameters	<code><username></code> The name of the user resource to re-enable
Examples	To re-enable a disabled user: <code>arcsight reenabler <username></code>

refcheck

Description	Resource reference checker
Applies to	Manager
Syntax	<code>refcheck</code>
Parameters	None
Examples	To run: <code>arcsight refcheck</code>

regex

Description	Graphical tool for regex-based FlexConnectors
Applies to	SmartConnectors
Syntax	<code>regex</code>
Parameters	None
Examples	To run: <code>arcsight regex</code>

replayfilegen

Description	Wizard for creating security event data files ("replay files") that can be run against a Manager for testing, analysis, or demonstration purposes. Note: This is a client side command only and should be executed from the Console's ARCSIGHT_HOME/bin directory.
Applies to	Console
Syntax	<code>replayfilegen -m mgr [parameters]</code>

Parameters	-f <file>	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
	-i <mode>	Mode: console, silent, recorderui, swing
Examples	Run from the Console's <ARCSIGHT_HOME>/bin directory:	
	arcsight replayfilegen	
	To run in console mode: arcsight replayfilegen -i console	

resetpwd

Description	Wizard to reset a user's password and optionally notify the user of the new password by e-mail	
Applies to	Manager	
Syntax	resetpwd	
Parameters	-f <file>	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
	-i <mode>	Mode: console, silent, recorderui, swing
	-h	Display command help
Examples	To reset a user's password: arcsight resetpwd	

resvalidate

Description	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. Make sure you stop the Manager before you run this command. If you have more than 50,000 actors you should first increase your Java heap size to 8 GB before running this command.	
Applies to	Manager, Database	
Syntax	resvalidate	
Parameters	-excludeTypes	Resource type to exclude from being checked;
	<exclude_resource_names>	for example, Rule, DataMonitor If specifying multiple resource types to exclude, use comma to separate them. Resource type – Rule,DataMonitor(comma separated)

	<p><code>-out <output_dir></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</p> <p><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 is reported as invalid but not marked invalid. However if <code>-persist=true</code>, the rule is marked as invalid. Default: <code>persist=true</code>.</p>
Examples	<p>In general, if you need to run the resource validation script, run it twice: the first time with <code>'-persist true'</code> (default) to validate and fix invalid resources, and the second time with <code>'-persist false'</code> to generate a correct report:</p> <pre>arcsight resvalidate arcsight resvalidate -persist false</pre>

ruledesc

Description	Rule description tool to fetch rules information. (Used by HPOVO.) Tool to monitor managed objects in the Manager	
Applies to	Manager	
Syntax	<code>ruledesc -t {ovo uri} -i info [parameters]</code>	
Parameters	<code>-t <type></code>	(Required) Type: { ovo uri }
	<code>-i <info></code>	(Required) Info (depends on type).
	<code>-m <host></code>	Manager host name or address
	<code>-p <pwd></code>	Password
	<code>-port <port></code>	Port for Manager. Default: 8443
	<code>-prot <prot></code>	Protocol {http https}. Default: https
	<code>-u <name></code>	User name
Examples	<p>To run:</p> <pre>arcsight ruledesc</pre>	

runcertutil

Description	<p>A wrapper launcher for the nss certutil tool used for managing certificates and key pairs. For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website.</p> <p>Note: If you do not see any error or warning messages after <code>runcertutil</code> has run, it is an indication that the command completed successfully.</p>
--------------------	---

Applies to	N/A	
Syntax	arcsight runcertutil	
Parameters	-A	Add a certificate to the database
	-a	Use ASCII format or allow the use of ASCII format for input or output.
	-v <certificate_validity_in_months>	<p>Set the number of months for which a new certificate is valid. You can use this option with the</p> <p>-w option which sets the beginning time for the certificate validity. If you do not use the -w option, the validity period begins at the current system time.</p> <p>If you do not specify the -v argument, the default validity period of the certificate is three months.</p>
	-w <beginning_offset_months>	Set an offset from the current system time, in months, for the beginning of a certificate's validity period. Can be used when creating the certificate. Use a minus sign (-) to indicate a negative offset. If this argument is not used, the validity period begins at the current system time.
	-n <certificate_name>	<p>Alias for the certificate</p> <p>Notes:</p> <ul style="list-style-type: none">• When generating a key pair on the Manager or ArcSight Web, it is mandatory to set the alias name to "mykey" (without the quotes)• When importing a certificate, you can set the alias name to any name of your choice
	-t <attributes>	Set the certificate trust attributes
	-d <certdb_dir>	Specify the directory of the certificate database relative to <ARCSIGHT_HOME>.
	-i	Certificate import request
	-L	List all the certificates
	-r	Encoding type
	-o <filename>	Output file name for new certificates or binary certificate requests. Be sure to use quotation marks around the file name if the file name contains spaces. If you do not specify a filename, by default, the output is directed to standard output.
	-S	Create a certificate to be added to the database
	-s <subject>	Subject name
	-k <key_type>	Type of key pair to generate

	-x	Self signed
	-m <serial_number>	Certificate serial number
	-v <days>	Validity period in days, for example, use -v 1825 to change the validity period to 5 years where 1825 is the number of days in 5 years.
	-V	Check the validity of the certificate
	-n <cert_name>	Certificate name
	-H	Help on this tool
Examples	To run: arcsight runcertutil	

runmodutil

Description	A wrapper launcher for the modutil nss cryptographic module utility. For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website.	
Applies to	N/A	
Syntax	arcsight runmodutil	
Parameters	-dbdir <dir_path>	The security database directory
	-H	Help on this tool
Examples	To run: arcsight runmodutil	

runpk12util

Description	The pk12util allows you to export certificates and keys from your database and import them into nssdb. This is a wrapper launcher for the pk12util nss tool. For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website.	
Applies to	N/A	
Syntax	arcsight runpk12util	
Parameters	-d <Cert_directory>	Path to your certificate directory (nssdb)
	-i <file>	The name of the file to be imported
	-h	Help on this tool

Examples	To run: arcsight runpk12util
-----------------	---------------------------------

script

Description	Run a Python script
Applies to	Manager
Syntax	script -f <script_file>
Parameters	-f <file_list> The script(s) to run
	-a <args> Command line arguments to pass to script
Examples	To run a Python script: arcsight script myScript.py

searchindex

Description	Utility that creates or updates the search index for resources. 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, manually configure the Manager to use the updated index.	
Applies to	Manager	
Syntax	searchindex -a action	
Parameters	-a <action>	Possible actions: create, update, or regularupdate create—Creates a new search index. update—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. regularupdate—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.
	-m <manager>	Name of the Manager
	-p <password>	Password for the user
	-t <time>	Time stamp that indicates starting when the resources should be updated
	-u <user>	User name with which to log in to the Manager
Examples	To run: arcsight searchindex -a <action>	



If you get an error in the server log for the `searchindexutility` that says `outofmemoryError`, you can increase the cap on the Java heap size. Go to your environment variables and increase the value for the variable called `ARCSIGHT_SEARCH_INDEX_UTILITY_JVM_OPTIONS`.

Set the variable like the following example:

```
ARCSIGHT_SEARCH_INDEX_UTILITY_JVM_OPTIONS="-Xms512m -Xmx8192m"
export ARCSIGHT_SEARCH_INDEX_UTILITY_JVM_OPTIONS
```

`Xms` is the initial Java heap size. `Xmx` is the maximum. The above values are the defaults.

When that variable is set, it takes priority over the default settings as well as `ARCSIGHT_JVM_OPTIONS`.

sendlogs

Description	Wizard to sanitize and save ArcSight log files so that you can send them to customer support for analysis, if they instruct you to do so. Note: it does not actually <i>send</i> the log files anywhere.	
Applies to	Manager, Database, Console	
Syntax	<code>sendlogs</code>	
Parameters	<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>-n <num></code>	Incident number (Quick mode)
Examples	<code>arcsight sendlogs</code>	

tee

Description	Displays the output of a program and simultaneously writes that output to a file	
Applies to	Manager	
Syntax	<code>-f <filename></code>	
Parameters	<code>-a</code>	Append to the existing file
Examples	To run: <code>arcsight tempca -i arcsight tee sslinfo.txt</code>	

tempca

Description	Inspect and manage demo certificates	
Applies to	Console	

Syntax	tempca	
Parameters	-a <alias>	Key store alias of the private key to dump
	-ac	Add the demo CA's certificate to the client truststore
	-ap	Create demo SSL key pair and add it to the Manager key store
	-dc	Dump/export the demo CA's certificate to a file (demo.crt) for browser import
	-dpriv	Dump private key from the Manager key store
	-f <file>	Filename to write the demo CA's certificate to
	-i	Display summary of current SSL settings
	-k <n>	Key store: Manager (1) or Web Server (2)
	-n <host>	Host name of the Manager (opt for the creation of a demo key pair)
	-nc	No chain: Do not include certificate chain (option for creation of a demo key pair)
	-rc	Reconfigure not to trust demo certificates. Removes the demo CA's certificate from the client truststore
	-rp	Remove pair's current key pair from the Manager key store
	-v <days>	Validity of the new demo certificate in days (Default: 365)
Examples	To run: arcsight tempca	

threaddumps

Description	Utility to extract and reformat thread dumps from the file to which you wrote the thread dumps in the managerthreaddump command (manager/logs/default/server.std.log). The output is an html file in the bin directory from which you run this command. It provides a list of links to all the thread dumps in a summary format.	
Applies to	Manager	
Syntax	threaddumps <file>	
Parameters	<filename>	Specify the name of the thread-dump file.
	-h	Display command help
Examples	To run: arcsight threaddumps	

tproc

Description	Standalone Velocity template processor	
Applies to	Manager	
Syntax	tproc	
Parameters	-d <file>	Definitions file
	-Dname=value	Defines
	-h	Display command help
	-l	Keep log file
	-o <file>	Output file
	-p <file>	Properties file
	-t <file>	Template file
	-v	Verbose mode
Examples	To run: arcsight tproc	

webserversetup

Description	See runwebsetup and websetup
Applies to	ArcSight Web

websetup

Description	Run the ArcSight Web Configuration Wizard
Applies to	ArcSight Web
Syntax	websetup
Parameters	None
Examples	To run the ArcSight Web Configuration Wizard: arcsight websetup

whois

Description	Script used by the whois command of the console
Applies to	Console

Syntax	<code>whois [-p <port>] [-s <host>] <target></code>	
Parameters	<code>-p <port></code>	Server port
	<code>-s <host></code>	Name or address of 'whois' server
	<code><target></code>	Name or address to lookup
Examples	To run: <code>arcsight whois</code>	

CORR-Engine ArcSight Commands

These commands are used to manage data in the CORR-Engine. They are located in `/opt/arcsight/logger/current/arcsight/logger/bin`.

To run a CORR-Engine ArcSight command script, open a command window and switch to the `/opt/arcsight/logger/current/arcsight/logger/bin` directory. These arcsight commands run using the file `arcsight.sh` in that location. The general syntax is as follows:

```
arcsight <command_name> [parameters]
```

configbackup

Description	The <code>configbackup</code> command backs up certain essential configuration information such as search settings and the configuration of archives (not the archives themselves). It places this backup in a file called <code>configs.tar.gz</code> which you can find in <code>opt/arcsight/logger/current/arcsight/logger/tmp/configs</code> .
Applies to	CORR-Engine
Syntax	<code>arcsight configbackup</code>
Parameters	none
Example	To run: <code>/opt/arcsight/logger/current/arcsight/logger/bin/arcsight configbackup</code>

Make sure you are familiar with these guidelines before you create a backup file:

The `configbackup` command creates the `configs.tar.gz` file, which you must then copy to a safe location.

Make a note of the following, which must match exactly on the machine to which you restore:

- Operating system and version
- Path to the archive locations for each storage group
- ESM version
- MySQL password

disasterrecovery

Description	This command restores the data backed up using the configbackup command.
Applies to	CORR-Engine
Syntax	arcsight disasterrecovery start
Parameters	start
Example	<p>To run:</p> <pre> /etc/init.d/arcsight_services stop logger_servers cp ~/configs.tar.gz /opt/arcsight/logger/current/backups/configs.tar.gz /opt/arcsight/logger/current/arcsight/logger/bin/arcsight disasterrecovery start /etc/init.d/arcsight_services start logger_servers </pre>

Make sure you are familiar with these guidelines before you restore a backup file:

- When you restore this data, the existing data is deleted.
 This command restores the specific settings that were current at the time the backup was taken. Any configuration settings that were updated between the time of the backup and the time of the restore are lost.
 This includes event data. The assumption is that you are restoring this configuration to a new, clean installation with no event data, or at least none that needs to be preserved.
- Restore the content to the same version of ESM that was used to create the backup file.
- Restore the content to the same version of the operating system as the one used to create the backup file.
- The archive locations for the backed-up storage groups must already exist and be the same.
- The MySQL password must be the same as on the machine from which you backed up.

exportdatausage

Description	<p>ESM keeps track of event counts and size from each connector. Use this command to export this event data as a comma-separated values (CSV) file. You can use this information to track the event throughput by connector.</p> <p>Note: This command has to be run from a different location than the other arcsight commands. Run it from: /opt/arcsight/logger/current/arcsight/logger/bin</p>
Applies to	CORR-Engine
Syntax	exportdatausage <path/file>

Optional Parameter	<path/file>	Specify the path and name of the CSV file to which to export the usage data. It can be a relative or absolute path. You do not need to specify the .csv extension.
		If you do not specify this parameter, the data is displayed on screen.
Examples	To create a file called usagefile.csv in /opt/arcsight, run: arcsight exportdatausage /opt/arcsight/usagefile	

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 Customer Support is available if you need it.

If you intend to have 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 137](#)
[“Query and Trend Performance Tuning” on page 139](#)
[“SmartConnectors” on page 141](#)
[“ArcSight Console” on page 142](#)
[“Manager” on page 144](#)
[“ArcSight Web” on page 144](#)
[“CORR Engine” on page 145](#)
[“SSL” on page 145](#)

General

Your License expired and you cannot start the ArcSight Command Center to specify a new license file.

Run the `arcsight managersetup` command as documented in [Chapter 4, Running the Manager Configuration Wizard, on page 83](#).

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 memory that it can cause the 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 virtual memory and heap, so the report

is more likely to generate successfully. Even if the memory allocated is still not enough, the report failure does 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 Manager in the `server.properties` file, set `report.canarchiveportinseparateprocess=true`. This makes a new report parameter available on the Console.
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight 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 does not consume the resources of the Manager's virtual memory.



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.

Scheduled rules take too long or time out

If you have a system, perhaps one with a high EPS, in which the scheduled rules are not running quickly enough, you can enable them to run in parallel (multi-threading) to speed them up. Add the following property to the `server.properties` file:

```
rules.replay.run.parallel=true
```

You can also set the number of threads to use, as follows (the default if you do not use this property is four threads):

```
rules.replay.numthreads=<number of threads to use>
```

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>/il18n/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. 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 Unix, the CMap path is relative to the Adobe Reader installation -- `<adobe_reader_dir>/Resource/CMap`.

E-mail notification doesn't happen

If you receive the following error:

```
[2009-12-03 14:31:33,890] [WARN
] [default.com.arcsight.notification.NotifierBase] [send] Unable to
send out e-mail notification, notifications have not been
configured.
```

- Verify the following properties are set in the `server.properties` file:


```
notifications.enable=true
```

and

```
notifications.incoming.enable=true
```
- Check `server.properties` file to find which SMTP server is associated with the Manager. Make sure that the SMTP server is up and running.
Review the Notification resource and confirm the e-mail address and other configuration settings.

Notification always escalates

Check `server.properties` file to find which POP3 or IMAP server is associated with the Manager. Make sure that the POP3 or IMAP server is up and running, in order to process acknowledgements from notification recipients.

Pager notification doesn't happen

Check `server.properties` file to find which SNPP server is associated with the Manager. Make sure that the SNPP server is up and running.

Query and Trend Performance Tuning

To improve query execution in high-EPS systems, various queries used by the trends in the default ESM system have been optimized. The scheduler allocates two threads for processing system tasks. This alleviates performance issues caused by conflicts between system tasks and user level tasks within the scheduler.

The following sections provide some troubleshooting tips.

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 times 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 uses 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 reflects 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 helps reduce scheduler and database contention.
- As trend data gathering tasks wake up, the trend attempts 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 does 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.

Disable these trends on high-throughput systems

If your system environment typically processes a very large number of events per second (EPS) (such as more than 1000 EPS or 100 million events per day), we recommend that you manually disable the following 9 trends, if their packages are installed:

`/All Trends/ArcSight Administration/ESM/User Access/ArcSight User Login Trends - Hourly (Installed by default)`

`/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 do you know when a trend is caught up?

You can use either of the following techniques, both using the ArcSight 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 does it take for a trend to catch up?

This depends on how long the underlying query interval is, but a trend typically does 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 returns no results (but it does not fail).

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 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 are lost.

SmartConnector not reporting events

Check the SmartConnector log for errors. If the SmartConnector cannot communicate with the Manager, it caches events until its cache is full.

ArcSight Console

Can't log in with any Console

Check that the Manager is up and running. If the Manager is not running, start it.

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 affects 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 cannot connect to the Manager

If you start an ArcSight Console that could previously connect to the Manager with no trouble, but now it can't, see if the error is similar to:

"Couldn't connect to manager - improper authorization setup between client and manager."

If so, it's likely that the manager has been reconfigured in such a way that it now has a new certificate. Especially if the Console asked you to accept a new certificate when you started it. To fix this, find and delete the certificate that the Console was using before, and then manually import another certificate from the Manager.

Console reports out of memory

If your ArcSight Console is so busy that it runs out of memory, change the memory settings in the `console.bat` or `console.sh` file. This file (for Windows or Linux, respectively) is located in the directory in which you installed the ArcSight Console, in `Console/current/bin/scripts`.

Find the line that starts with `set ARCSIGHT_JVM_OPTIONS=` and change the parameter `-Xmx512m` to `-Xmx1024m`. Xmx is the maximum JVM memory

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 Customer Support.

The Manager Status Monitor reports an error

The Console monitors the health of the 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 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 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.

Duplicate audit events or rule actions after a crash recovery

When you stop ESM, it takes a checkpoint of the rules engine so that it knows where it stopped. If ESM crashes in such a way that it cannot take a checkpoint (power failure, for example), it returns to the last checkpoint when it restarts, and replays events from there. Any actions that occurred between that checkpoint and the ESM crash will therefore be repeated. Repeated actions that generate audit events generate duplicate audit events.

You should investigate repeated actions that do not duplicate well. For example, if an action adds an item to an Active List, that item's counter will be incremented. If the action runs a command, it will run it again, and so on.

You can reduce duplicates by including a rule condition that checks if the relevant entry is already in the active list.

Console does not start in Windows 2008

If you installed and then started the Console in Windows 2008, you may get an error due to access refusal. In Windows 2008, make sure to configure the User Access Control (UAC) of the ArcSight Console user. Consult the Microsoft web site for more details on UAC specific to Windows 2008.

Case data fields appear blank

A number of case fields accept up to 4,000 bytes. However, if you fill too many such fields to the maximum, then you can exceed the limit and the fields can appear blank when you view the case.

This is because of a database limitation on the size of a row (a case, for example), which is about 8k bytes. For large fields, only 768 bytes are stored in the row, along with a 20 byte pointer to the rest, which is stored outside the table. This enables you to have considerably more than 8K of data, but you can still exceed the limit for the database row for a resource.

As a guideline, keep the number of large fields in a case (or other resource with large fields) below ten. The data in the smaller fields contributes to the total, so if you still encounter the problem, consider them as well.

Manager

Can't start Manager

The Manager provides information on the command console which may suggest a solution to the problem. Additional information is written to

<ARCSIGHT_HOME>/logs/default/server.std.log.

Manager shuts down

The Manager stops when it encounters a fatal error. The file

<ARCSIGHT_HOME>/logs/default/server.std.log has more details about the error condition.

SmartConnectorServices do not start after a power failure during “start all”

An unexpected power-off during services startup may result in unavailable postgres, logger, and manager services. Those services might not start even after rebooting the server.

To resolve the problem, delete the locked postgres file. The location of the locked file, is given in the postgres log file in /opt/arcsight/logger/data/postgres/serverlog.

Reboot the server after removing the locked file.

Switching between daylight savings and standard time can skip a scheduled task

- If the trigger time for a particular scheduled task run happens to fall during the transition time from DST to ST or vice versa, the interval for that particular run gets thrown off. The interval calculation for subsequent scheduled runs do not get affected.
- Currently, there are four time zones that are not supported in ESM:
 - ◆ Kwajalein
 - ◆ Pacific/Kwajalein
 - ◆ Pacific/Enderbury
 - ◆ Pacific/Kiritimati

These time zones fall in two countries, Marshall Islands and Kiribati.

ArcSight Web

Some content, particularly dashboards, is not visible

Install the latest Adobe Flash plug-in to your browser. Visit the Adobe web site 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 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 affects 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 is disabled.

Can't start ArcSight Web

If the ArcSight Web Server cannot start, check that the Manager is up and running. If the Manager is not running start it.

Examine the ArcSight Web log file for specific error messages. If the message is not clear, contact HP Customer Support.

CORR Engine

Temporary sort space limit exceeded

Under some circumstances you can get an error that includes the following:

```
Encountered persistence problem while fetching data: Unable to
execute query: Temporary sort space limit exceeded
```

Possible solutions include eliminating unnecessary trends, if any, avoid running too many at the same time, and trim queries to return more refined data sets. If the problem persists, try increasing the value of `sort_temp_limit` in `/opt/arcsight/logger/data/mysql/my.cnf`.

For information on creating queries, trends, and reports, refer to the "Building Reports" chapter in the ArcSight Console User's Guide.

If increasing the `sort_temp_limit` is insufficient, and the following circumstance applies, there are two additional remedies.

Excessive temporary file space gets used when Group By (or sorting) is performed on the Event table. If you use Group By (or sorting), use the ArcSight substring function on varchar/string event fields to minimize the data manipulation during grouping. You can use existing local or global variables to achieve this behavior and replace the existing field in the query with the variable. Search in the ArcSight Console User's Guide, in the "Reference Guide" section, for information in variables and substrings.

If the file space usage is still not satisfactory, you can convert the character set automatically to Latin which uses less space. To do so, set the `event.query.charset.conversion` property to 1 in the `/opt/arcsight/manager/config/server.properties` file to convert the existing character set to latin1. Alternatively, set the property to 2 for conversion to binary and then to Latin (to minimize conversion error for non-English character set). The default value of this property is 0 (zero).

If you use this conversion on multi-byte character sets, it will truncate the characters to single-byte Latin characters, which is likely to render them meaningless. So only use this approach if it's appropriate.

SSL

Cannot connect to the SSL server: IO Exception in the server logs

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.
- 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. To check the certificate's valid date range see ["Viewing Certificate Details From the Store" on page 57](#).

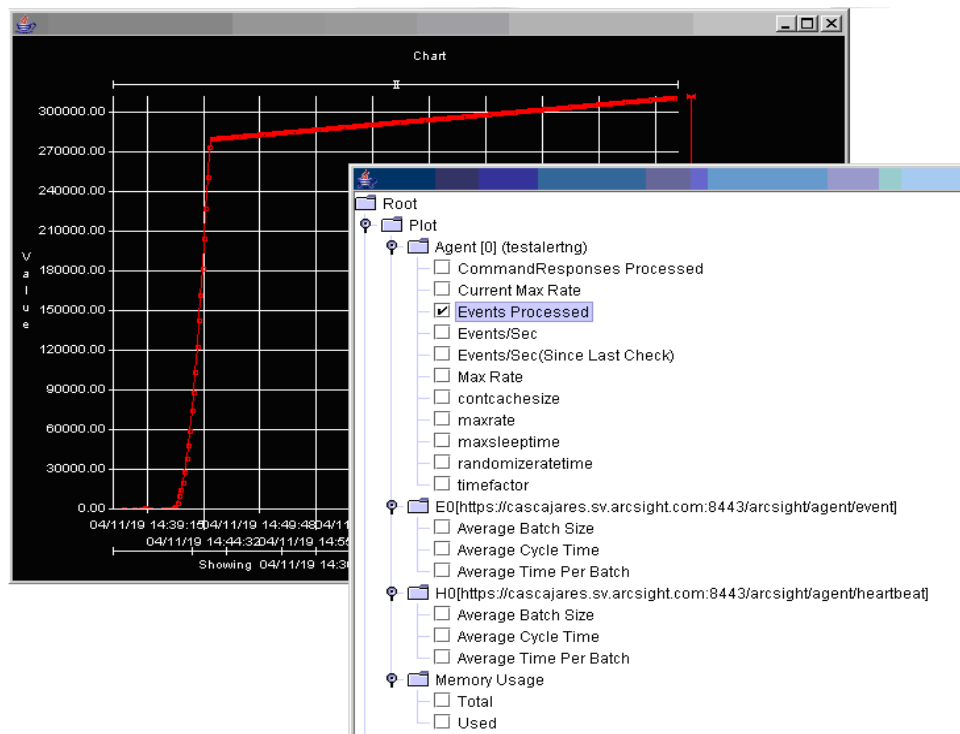
Appendix C

The Logfu Utility

This appendix is divided into the following sections:

- “Running Logfu” on page 150
- “Example” on page 152
- “Troubleshooting” on page 152
- “Menu” on page 154
- “Typical Data Attributes” on page 154
- “Intervals” on page 155

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.



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` switches tell it which file names to look for. The `-m` switch tells it to look for all three Manager logs—`server.std.log`, `server.log`, and `server.status.log`—for example.

To run Logfu, follow these steps:

- 1 Open a command or shell window in `<ARCSIGHT_HOME>/logs/default`. This refers to the logs directory under the ArcSight installation directory. Logfu requires an X Windows server on Unix platforms.
- 2 Run logfu for the type of log to 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.

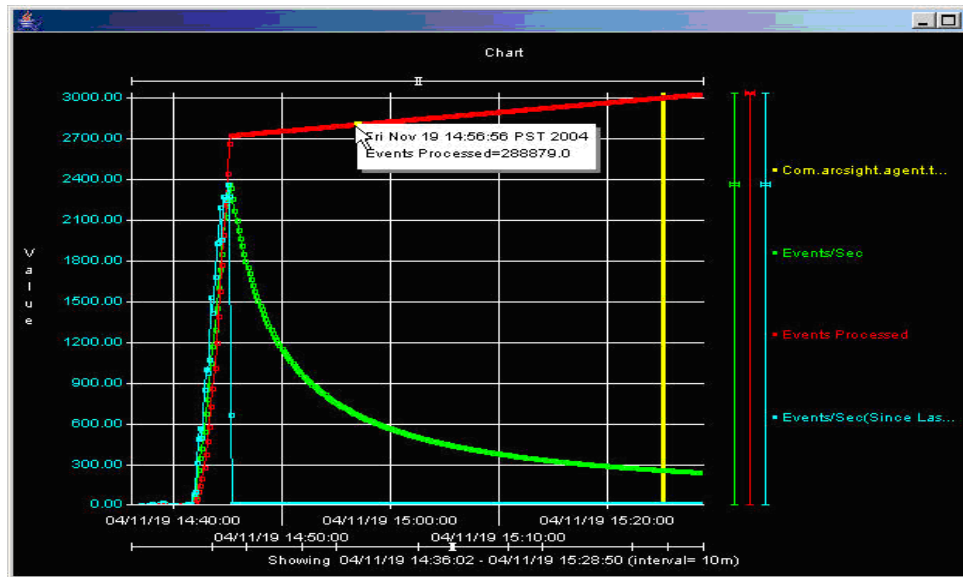
The initial display is always an empty grid. Loading very large log files can take a few minutes (a 100MB log might take 5 or 10 minutes). Once log files are scanned, the information gleaned from them is cached (in files named `data.*`), which speeds up loading the second time. If something about the 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.



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 fills 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 the figure, above.

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). A sample HTML report is shown below.

Logfu

Analizers

Name	agent.log	Path	null/	Elapsed	0 mins 2 secs 203 ms
				Total	0 mins 2 secs 203 ms

Sessions by Length

[1]	00:00:48:16:869	[0]	00:00:04:24:631
-----	-----------------	-----	-----------------

Sessions by Throughput

[0]	0.0	[1]	0.0
-----	-----	-----	-----

Sessions by Exception count

[0]	0	[1]	0
-----	---	-----	---

Sessions by longest Full GC

All Sessions

[0]	[1]
-----	-----

Session 0

Start	04-11-19 14:35:17	ArcSightBuildVersionInfo	r_11-8-2008_20:17:33
End	04-11-19 14:39:41	ArcSightSystemVersion	3.0.1.0.0
Length	0 days 0 hrs 4 mins 24 secs	Event Transport [0]	https://ca:8443/arcsight/agent/event
log filename	agent.log	Heartbeat Transport [0]	https://ca:8443/arcsight/agent/heartbeat
Throughput	0.0		
Avg Insert Threads	0.0		

Menu

Menu Item	Description
Show Plot/Event Window	Presents the possible attributes to be displayed
Bring To Front, Send to Back, Undo Zoom, Zoom out	Return to previous view
Auto Scale	Fit all data on the grid
Save as JPG	Save a snapshot of the current view on the grid
Go to	Display the line of the log file which corresponds to a particular data point
Reset	Clear all checked attributes and restore the normal startup view of an empty grid
Preferences	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	
Events/Sec (Since Last Check)	Averaged events per second
Max Rate	Events per second in last minute (unless check time is configured to a different interval)
contcachesize	
maxrate	Contiguous Cache Size
maxsleeptime	Maximum Rate
randomizeratetime	Maximum Sleep Time
timefactor	Randomize Rate Time

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 D

Creating Custom E-mails Using Velocity Templates

This appendix describes how to modify Velocity templates to customize e-mail messages you receive from the ArcSight notification system.

This appendix is divided into the following sections:

[“Overview” on page 157](#)

[“Notification Velocity Templates” on page 157](#)

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.

ESM supports the use of *velocity templates* or scripts as defined by The Apache Velocity Project (<http://velocity.apache.org/>). Velocity templates are a means of specifying dynamic or variable inputs to, or outputs from, underlying Java code.

Velocity templates are an advanced user feature.

- Because Velocity templates have such wide-ranging and intricate possibilities, mis-application or inappropriate application is entirely possible. HP cannot assume responsibility for adverse results caused by user-supplied Velocity templates.
- HP ArcSight does not provide error checking or error messaging for user-created velocity expressions. Refer to the Apache Velocity Project web page at <http://velocity.apache.org/> for more information on using velocity templates.

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
```

Using Email.vm and Informative.vm Template Files

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/Snort.vm

-----
```

Once you have created the secondary templates, you can edit the `Email.vm` template to insert conditions that 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 generate:

```
Notification ID: fInjoQwBABCGMJkA-a8Z-Q== Escalation Level: 1

=== Complete Event Details ===

Threat Details

Event:                      Internal to External Port Scanning
Description:                Internal to External Port Scanning Activity
Detected; Investigate Business Need for Activity

Severity:                   2

-----

Source Details

Source Address:             10.129.26.37

Source Host Name:

Source Port:                0

Source User Name:          jdoe

-----

Target Details

Target Address:             161.58.201.13

Target Host Name:

Target Port:                20090

Target User Name:

-----

Extra Information (where applicable)

Transport Protocol:        TCP

Base Event Count:          1

Template:
/home/arcsight/arcsight/Manager/config/notifications/Snort.vm

-----

How to Respond
```

This message can be acknowledged in any of the following ways:

- 1) Reply to this email. Make sure that the notification ID listed in this message is present in your reply)
- 2) Login to the ArcSight Console and click on the notification button on the status bar
- 3) Login to myArcSight and go to the My Notifications Acknowledgment page at
<https://mymanager.mycompany.com:9443/arcsight/app?service=page/NotifyHome>

View the full alert at

<https://mymanager.mycompany.com:9443/arcsight/app?service=page/NotifyHome>

Symbols

#if statement 158

A

- access control list (ACL) 90
- ACLReportGen command 99
- Active Directory, setting up authentication for 91
- actors
 - configuring 42
- agent logfu command 99
- agent tempca command 100
- agentcommand command 100
- agentsvc command 101
- agenttempca command 101
- agentup command 101
- anti-virus scan impact 11
- arcdt command 101
- archive
 - task syntax 109
- archive command 103
- archivefilter command 110
- ArcSight Console
 - adjust memory 18
 - session timeout 29
- ArcSight Express Appliance
 - configuring 83
- ArcSight Web
 - session timeout 29
- authentication 89
 - Active Directory 91
 - built-in 90
 - custom JAAS plug-in configuration 92
 - external 89
 - LDAP 92
 - password-based 90
 - PKCS#11 89
 - RADIUS 90
 - SSL client-only 93
 - using certificates 79

B

- bleep command 111
- bleepsetup command 112
- built-in authentication 90

C

- CA-signed certificate 62
 - import 63
 - obtaining 62

- certificate
 - migrating type-to-type 77
- changepassword command 112
- character set in passwords 30
- checklist command 112
- Cipher suite
 - default mode 50
- cipher suites 50
- client keystore 93
- commands
 - ACLReportGen 99
 - agent logfu 99
 - agent tempca 100
 - agentcommand 100
 - agentsvc 101
 - agenttempca 101
 - agentup 101
 - arcdt 101
 - archive 103
 - archivefilter 110
 - bleep 111
 - bleepsetup 112
 - changepassword 112
 - checklist 112
 - console 112
 - consolesetup 113
 - downloadcertificate 114
 - exceptions 114
 - export_system_tables 115
 - exportdatausage 135
 - flexagentwizard 115
 - groupconflictingassets 116
 - id defensesetup 116
 - import_system_tables 117
 - keytool 117
 - keytoolgui 118
 - kickbleep 118
 - listsubjectdns 118
 - logfu 118
 - managerinventory 119
 - manager-reload-config 120
 - managersetup 120
 - managertreaddump 121
 - managerup 121
 - monitor 121
 - netio 122
 - package 122
 - portinfo 124
 - reenableuser 125
 - refcheck 125
 - regex 125

- replayfilegen 125
- resetpwd 126
- resvalidate 126
- ruledesc 127
- runcertutil 127
- runmodeutil 129
- runpk12util 129
- script 130
- searchindex 130
- sendlogs 131
- tee 131
- tempca 131
- threaddumps 132
- tproc 133
- webserversetup 133
- websetup 133
- whois 133
- compression mode 37
- configuration
 - Manager logging 20
 - SNMP trap sender 38
- configuring
 - SSL 91
- console command 112
- consolesetup command 113
- custom authentication scheme 92

D

- diagnostic information 22
- downloadcertificate command 114
- dynamic properties 15

E

- Email.vm file
 - contents 158
 - elements 158
 - how it works 159
- encryption 50
- events
 - send as SNMP trap 38
- exceptions command 114
- export_system_tables command 115
- exportdatausage command 135
- external authentication 89
 - guidelines 89

F

- failed logins, restricting 33
- flexagentwizard command 115

G

- groupconflictingassets command 116

H

- hostname
 - in web console URL 11

I

- idensesetup command 116
- import_system_tables command 117

- Informative.vm file
 - contents 158
 - elements 158
 - how it works 159
- IP address
 - in web console URL 11

J

- JAAS plug-in authentication 92

K

- keytool command 117
 - detailed usage 80
- keytoolgui command 118
- kickbleep command 118

L

- LDAP
 - setting up authentication for 92
- license
 - file import 20
- license expired 137
- listsubjectdns command 118
- logfu
 - command 118
 - data attributes 154
 - Example 152
 - example 108
 - intervals 155
 - menu 154
- login
 - restricting failures 33
- logs
 - gathering 22

M

- Manager
 - change ports 29
 - change properties dynamically 17
 - decoupled process execution 9
 - Password Configuration 29
 - reconfigure 28
 - reconnect 10
- managerinventory command 119
- manager-reload-config command 120
- managersetup command 120
- managereadddump command 121
- managerup command 121
- memory, adjust 18
- monitor command 121

N

- netio command 122
- notification velocity templates 157

P

- package command 122
- password-based authentication 90
- passwords
 - and character sets 30

- check with regular expressions 31
- guidelines 30
- set expiration 32
- PKCS#11 authentication 89
- port, Manager, changing 29
- portinfo
 - command 124
- properties file
 - change dynamically for Manager 17
 - editing 14
 - format 13
 - secure 18

R

RADIUS

- setting up authentication for 90
- reenableuser command 125
- refcheck command 125
- regex command 125
- replayfilegen command 125
- resetpwd command 126
- resources
 - import from archive 108
- resvalidate command 126
- ruledesc command 127
- runcertutil command 127
- runmodutil command 129
- runpk12util command 129

S

- script command 130
- searchindex command 130
- send logs
 - utility 21
- sendlogs
 - command 131
- SmartConnectors
 - event compression 37
 - start 11
- SNMP trap, send events as 38
- SSL

- client-only authentication 93
- configuring 91, 92
- SSL authentication
 - CA-signed certificate 62
 - certificate 53
 - how it works 51
 - self-signed certificate 58
 - setup 67
 - verify certificate use 78

T

- tee command 131
- tempca 80
- tempca command 131
- template files 159
 - customizing 160
- threaddumps command 132
- tproc command 133
- troubleshooting
 - general 137
 - logfu 152
 - manager 144
 - SSL 145
- turbo mode 37

U

- users
 - re-enabling account 33

V

- velocity templates
 - notification 157

W

- webserversetup command 133
- websetup command 133
- whois
 - command 133

