



HP ArcSight ESM

Software Version: 6.9.0c

Administrator's Guide

July 10, 2015

Legal Notices

Warranty

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.

The information contained herein is subject to change without notice.

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

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.

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

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

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

Support

Contact Information

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

Contents

Chapter 1: Basic Administration Tasks	9
Starting Components	9
Starting the ArcSight Manager	9
Decoupled Process Execution	9
Stop Services Before Rebooting the ESM Server	10
Stopping the ArcSight Manager	10
Starting the ArcSight Console	10
Reconnecting ArcSight Console to the Manager	10
Starting the ArcSight Command Center	11
Starting ArcSight SmartConnectors	11
Reducing Impact of Anti-Virus Scanning	11
License Tracking and Auditing	12
Licensed EPS Compliance	12
ArcSight System Tasks	13
Setting up a Custom Login Banner	14
Chapter 2: Configuration	15
Managing and Changing Properties File Settings	15
Property File Format	15
Defaults and User Properties	15
Editing Properties Files	16
Dynamic Properties	17
Example	18
Changing Manager Properties Dynamically	19
Changing the Service Layer Container Port	20
Securing the Manager Properties File	20
Adjusting Console Memory	21
Adjusting Pattern Discovery	21
Improving Annotation Query Performance	22
Installing New License Files Obtained from HP	22
Configuring Manager Logging	23
Sending Logs and Diagnostics to HP Support	24
Guidelines for Using the sendlogs Command	24

Gathering Logs and Diagnostic Information	25
Reconfiguring the ArcSight Console After Installation	27
Reconfiguring ArcSight Manager	28
Changing ArcSight Command Center Session Timeout	28
Managing Password Configuration	28
Enforcing Good Password Selection	28
Password Length	28
Restricting Passwords Containing User Name	29
Password Character Sets	29
Requiring Mix of Characters in Passwords	29
Checking Passwords with Regular Expressions	30
Password Uniqueness	31
Setting Password Expiration	31
Restricting the Number of Failed Log Ins	32
Disabling Inactive User Accounts	32
Re-Enabling User Accounts	33
Advanced Configuration for Asset Auto-Creation	33
Asset Auto-Creation from Scanners in Dynamic Zones	33
Create Asset with Either IP Address or Host Name	33
Preserve Previous Assets	35
Changing the Default Naming Scheme	36
Compression and Turbo Modes for SmartConnectors	36
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	41
Deleting an Asset	41
Amortize Model Confidence with Scanned Asset Age	41
Tuning for Supporting Large Actor Models	42
About Exporting Actors	43
Setting Up ESM for MSSP Environments	43
Chapter 3: SSL Authentication	44
SSL Authentication Terminology	44

How SSL Works	48
Certificate Types	49
SSL Certificate Tasks	50
Export a Key Pair	51
Exporting a Key Pair Using keytool	51
Exporting a Key Pair Using keytoolgui	51
Import a Key Pair	52
Importing a Key Pair Using keytool	52
Importing a Key Pair Using keytoolgui	52
Export a Certificate	53
Exporting a Certificate Using keytool	53
Exporting a Certificate Using keytoolgui	53
Import a Certificate	54
Importing a Certificate Using keytool	54
Importing a Certificate Using keytoolgui	54
Creating a Keystore	55
Creating a Keystore Using keytool	55
Creating a Keystore Using keytoolgui	56
Generating a Key Pair	57
Generating a Key Pair Using keytool	57
Generating a Key Pair Using keytoolgui	57
View Certificate Details From the Store	57
Viewing a Certificate Details from the Store Using keytool	58
Viewing a Certificate Details from the Store Using keytoolgui	58
Delete a Certificate	58
Deleting a Certificate Using keytool	58
Deleting a Certificate Using keytoolgui	59
Using a Self-Signed Certificate	59
When Clients Communicate With One Manager	59
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
Sending a CA-Signed Certificate Using keytool	63
Sending a CA-Signed Certificate Using keytoolgui	64
Import the CA Root Certificate	64
Import the CA-Signed Certificate	65
Restart the Manager	68
Accommodating Additional Components	68

Removing a Demo Certificate	69
Replacing an Expired Certificate	69
Establishing SSL Client Authentication	69
Setting up SSL Client-Side Authentication on ArcSight Console	70
Setting Up Client-Side Authentication for ACC	74
Setting up Client-side Authentication on SmartConnectors	75
Migrating From One Certificate Type to Another	76
Migrating from Demo to Self-Signed	76
Migrating from Demo to CA-Signed	77
Migrating from Self-Signed to CA-Signed	77
Verifying SSL Certificate Use	77
Sample Output for Verifying SSL Certificate Use	78
Using Certificates to Authenticate Users to ArcSight	78
Using the Certificate Revocation List (CRL)	79
Chapter 4: Running the Manager Configuration Wizard	80
Running the Wizard	80
Authentication Details	82
How External Authentication Works	82
Guidelines for Setting Up External Authentication	82
Password Based Authentication	83
Built-In Authentication	83
Setting up RADIUS Authentication	83
Setting up Active Directory User Authentication	84
Configuring AD SSL	85
Setting up LDAP Authentication	85
Configuring LDAP SSL	86
Using a Custom Authentication Scheme	86
Password Based and SSL Client Based Authentication	86
Password Based or SSL Client Based Authentication	86
SSL Client Only Authentication	87
Appendix A: Administrative Commands	88
ArcSight_Services Command	88
ArcSight Commands	89
CORR-Engine ArcSight Commands	134

Appendix B: Troubleshooting	137
General	137
Pattern Discovery Performance	139
Query and Trend Performance Tuning	140
SmartConnectors	141
ArcSight Console	142
Case Data Fields Appear Blank	143
Manager	144
CORR Engine - Temporary Sort Space Exceeded	146
SSL	146
Appendix C: Creating Custom E-mails Using Velocity Templates	149
Velocity Templates	149
Notification Velocity Templates	149
Commonly Used Elements in Email.vm and Informative.vm Files	150
The #if statement	150
Contents of Email.vm and Informative.vm	150
Using Email.vm and Informative.vm Template Files	151
Understanding the Customization Process	151
Customizing the Template Files	152
Sample Output	153
Appendix D: Configuration Changes Related to FIPS	155
Tools Used to Configure Components in FIPS	155
FIPS Encryption	156
Types of Key Pairs Used in FIPS Mode	156
Types of Certificates Used in FIPS Mode	156
Using a Self-Signed Certificate	157
Using a Certificate Authority (CA) Signed Certificate	157
Steps Performed on the Manager	157
Steps Performed on the ArcSight Console	159
Some Often-Used SSL-Related Procedures	159
Generating a Key Pair in a Component's NSS DB	159
On the Manager	160
On the Console	160
Verifying Whether the Key Pair Has Been Successfully Created	161

Viewing the Contents of the Manager Certificate	161
Exporting Certificates	162
Exporting a Certificate From the Manager	162
Exporting a Certificate From the Console	162
Importing a Certificate into the NSS DB	162
On the Manager	163
On the Console	163
Importing an Existing Key Pair into the NSS DB	163
Setting up Server-Side Authentication	164
Setting up Client-Side Authentication	164
Changing the Password for NSS DB	165
Listing the Contents of the NSS DB	166
Viewing the Contents of a Certificate	167
Setting the Expiration Date of a Certificate	167
Deleting a Certificate from NSS DB	167
Replacing an Expired Certificate	168
Using the Certificate Revocation List (CRL)	168
Configuration Required to Support Suite B	169
Generating a Key Pair on the Manager	170
Exporting the Manager's Certificate	171
Importing a Certificate into the Manager	171
Changing a Default Mode Installation to FIPS 140-2	172
Manager	172
ArcSight Console	174
Connectors	176
Configure Your Browser for FIPS	176
Send Documentation Feedback	177

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.

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 Users Guide or the ArcSight Console Users Guide. Helpful topics in the ArcSight Console include:

- Managing User's and Permissions
- Modeling the Network
- Filtering Events
- Managing Resources
- Managing SmartConnectors
- Managing Partitions

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 run a very large report. 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 executor, 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
```

Stop Services Before Rebooting the ESM Server

Before performing a reboot run the following command as the user *arcsight*:

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

Performing a clean shutdown of services in this way will ensure the integrity of your ESM databases.

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 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 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 only 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 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.

Note: For the ESM Express Appliance, the only feature monitored is EPS.

Licensed EPS Compliance

Note: Licensed EPS compliance monitoring is not supported on the ESM Express appliance

By default, your events per second (EPS) throughput is monitored once every 24 hours and an average EPS value is calculated for that period. Your license places a limit on this average. It also places a limit on the number of times you are allowed to exceed the EPS limit over a period (rolling window) of days. In a given window, each time your EPS throughput exceeds the licensed limit, this violation is recorded. When the violations exceed the number allowed, your installation becomes noncompliant and you are temporarily prevented using certain functionality (as listed below).

For example, suppose your license is set up as follows:

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

If you exceed your maximum EPS limit (1,000) more than five times in seven days, punitive action starts.

The punitive action is that access to the resources in the following list is disabled for an hour for every day you've exceeded the EPS limit in the seven day period, up to a maximum of five hours. It starts as soon as you exceed your limit.

The EPS license compliance is enforced on the following viewers.

- Channels (event and resource channels)
- Data monitors
- Query viewers and query viewers in dashboard
- Pattern Discovery (creating new snapshots). **Note:** Pattern Discovery is not supported on the ESM Express appliance.
- Event graph from channel
- Global or Political Image Viewer in the Active Channel view
- Category model view
- Custom view Dashboards on the Console, but not the ArcSight Command Center

Nothing happens to any of the above viewers if they already exist in viewer table when you exceed the License limit. However, if you attempt to create a new viewer, stop and restart a channel, create or edit a data monitor, and so on, you get an error message dialog that you have exceeded your license.

As days continue to elapse, when the EPS limit violation is calculated to be five times or less in the past seven days, you become compliant and the features are automatically re-enabled.

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 indexes 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.

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
config/server.defaults.properties	config/server.properties	Manager Configuration

Default Properties	User Properties	Purpose
config/console.defaults.properties	config/console.properties	ArcSight Console Configuration
config/client.defaults.properties	config/client.properties	ArcSight Common Client 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, 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)
	9090	ESM Service Layer Container Port
	9000	Used by the Manager for peering.
TCP	8443	SmartConnectors, ArcSight Command Center, and ArcSight Console to Manager communication
TCP	636	Manager to LDAP server (with SSL if enabled)
TCP	389	Manager to LDAP server (without SSL if enabled)
TCP	143	Manager to IMAP server (for Notifications)
TCP	110	Manager to POP3 server (for Notifications)

Protocol	Port	Configuration
UDP/TCP	53	ArcSight Console to DNS Server communication (<code>nslookup</code> tool)
UDP/TCP	43	ArcSight Console to Whois Server communication (<code>whois</code> 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`
- `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, after 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 the administrator 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
```

Note: The `-diff` option compares all server properties—default and user properties. For all options available with the `manager-reload-config` command, see ["Administrative Commands" on page 88](#).

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:

- 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.

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

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

Adjusting Console Memory

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

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

Adjusting Pattern Discovery

Note: Pattern Discovery is not supported on the ESM Express appliance.

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 supersede 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, 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 114](#).

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.
<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>managersetup</code> command.

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 `sendlogs` command automatically locates the log files and compresses them. You can send the compressed files to Customer Support. For details on the `sendlogs` command, see ["Administrative Commands" on page 88](#).

- You can run this command 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 ["Administrative Commands" on page 88](#).

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

Guidelines for Using the `sendlogs` Command

When using the `sendlogs` command:

- 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 `sendlogs` command 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 `sendlogs` command on SmartConnectors, it gathers logs and diagnostic information (if applicable) for only those components. However, when you run this utility on ArcSight Console or Manager, you can gather logs and diagnostic information for all or a selected set of ESM components.

To run this command 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 the Console or Manager machine:

```
./arcsight sendlogs
```

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

Note: The Send Logs wizard remembers most of the choices you make when you run it for the first time. Therefore, for subsequent runs, if you choose to use the previous settings, you 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.

Choose either **Use current setting to gather logs** or **Change/Review settings before gathering logs**.

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 the next page](#).

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

Choose either **Local Logs Only** or **Logs from other components (Requires Manager credentials)**. These choices allow you to select whether you want only the local (the component from where you ran the sendlogs command) logs selected or to select logs from other components to be collected as well.

Local logs only:

If you select **Local logs only**, you can choose either **Include all time ranges** or **Choose a specific time range**.

If you select **Include all time ranges**, go to the step ["Sanitize logs" on the next page](#).

If you select **Choose a specific time range**, you are prompted to enter a **Start Time** and **End Time**, which is a time range for which the wizard gathers the logs.

Go to the step ["Sanitize logs" on the next page](#).

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 (for example, Manager, or Connectors) and the time range for which you want to gather logs. In addition, select whether you want to run the diagnostic utilities to gather additional information for those components.

If you choose to specify the diagnostic utilities to run, you are prompted to select the utilities from a list in a later screen. The diagnostic utilities you can select are described in ["arcdt" on page 92](#).

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

Note: 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 sendlogs Command](#)" on page 24.

If you choose **Do not sanitization logs (fastest)**, go to the step "[Incident Number](#)" below

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](#)" below.

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 `sendlogs` command 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. After 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 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 launches.

Reconfiguring ArcSight Manager

To reconfigure Manager settings made during installation, run the Manager Configuration Wizard. The Manager Configuration Wizard is covered in ["Running the Manager Configuration Wizard" on page 80](#).

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. If a property exists in both the `server.defaults.properties` file and the `server.properties` file, the value in the `server.properties` file is used. These files are located in `<ARCSIGHT_HOME>/config`. Values in the `server.properties` file supersede

Changing ArcSight Command Center Session Timeout

ArcSight Command Center will automatically log out if it has been inactive for a certain amount of time. This duration is defined by the configurable `tservice.session.timeou` property. If the session duration is too short, increase the value set for the `service.session.timeout` property in the `<ARCSIGHT_HOME>/config/server.properties` 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 15](#). 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.

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 more difficult to guess and can prevent 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.

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

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

- `auth.password.regex.match= /^\d.*\d$/`

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

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

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

- At least two upper case letters
 - At least two lower case letters
 - At least two digits
 - At least two special characters (no digits or letters)
- `auth.password.regex.reject= ^(?=[A-Z].*[A-Z])(?=[a-z].*[a-z])(?=[0-9].*[0-9])(?=[^a-zA-Z0-9].*[^a-zA-Z0-9]).{12,}$`

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

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

Password Uniqueness

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

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

If set to true, the Manager checks all other passwords to make sure nobody is already using the same password.

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

Setting Password Expiration

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.

After 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 reenableuser username
```

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

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`.

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.

Example	Action taken if previous asset with similar information and preserve = true
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 for SmartConnectors

These sections discuss compression techniques and turbo modes for SmartConnectors.

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.defaults.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.

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

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 (/All Filters/ArcSight System/Event Types/ArcSight Correlation 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 scheduled task that disables any scanned asset that has reached the specified age. By default, after 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 enable 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
```

Note that the default value -1 means that asset aging is turned off, not that assets will be disabled.

The value is expressed in days that define how long an asset is allowed to age before it is disabled. For example:

```
asset.aging.daysbeforedisable = <number of days>
```

So, this setting:

```
asset.aging.daysbeforedisable = 4
```

means that after 4 days, assets will be considered old and disabled. Set this property to a reasonable value that makes sense for your assets.

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
```

Verify that this property is set to `delete` for deletion of aging assets to occur.

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 port 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
240	0

Tuning for Supporting Large Actor Models

Note: The ESM Express appliance does not support Actors functionality.

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.

Note: In-memory capacity changes made to `arc_session_list` must match `sessionlist.max_capacity` in `server.properties`

If you update the in-memory capacity for the `arc_session_list` table to number other than the default 500,000, the value you enter must match the value set for `sessionlist.max_capacity` in `server.properties`.

2. **Adjust Java Heap Memory Size** using the Manager Configuration Wizard. 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. The Manager Configuration Wizard is covered in ["Running the Manager Configuration Wizard" on page 80](#).
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](#).

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 with the `-s` parameter, which specifies the export of session list data. Additionally, the `-s` parameter captures the special session list infrastructure that is part of the Actor Resource Framework in addition to the actor resources themselves.

Setting Up ESM for MSSP Environments

To set up ESM in a managed security service provider (MSSP) environment, do the following:

- Set up Customers. See the ArcSight Console User's Guide for details.
- Disable the search auto-complete feature. To do this, in the `logger.properties` file change the value of `auto-complete.fulltext.enabled` to **false**.

Chapter 3: SSL Authentication

This chapter describes the Secure Socket Layer (SSL) technology used for communication between the Manager and its clients—Console and SmartConnectors. It is not used between the Manager and the database.

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.

SSL Authentication Terminology

Terms that 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 48.

- **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.

- **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
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 either the `keytool` or `keytoolgui` command to view a truststore. See ["View Certificate Details From the Store" on page 57](#) for details on viewing 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 48](#).

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
Manager	truststore[2]	<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.

- **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` command, as described in ["Administrative Commands" on page 88](#).

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.encrypted</code>
Manager*	<code>server.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.

Whenever you change a password for the truststore, you must make the same change in the password entry in the corresponding properties file.

• 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 *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*	<code>client.properties**</code>	<code>ssl.keystore.password</code>
Manager	<code>server.properties</code>	<code>server.privatekey.password.encrypted</code>
Connector	<code>agent.properties**</code>	<code>ssl.keystore.password.encrypted</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.

Whenever you change a password for the keystore, you must make the same change in the password entry in the corresponding properties file.

- **NSS database password**

The default password for the Manager's nssdb and the Console's nssdb.client are both *changeit*. To change it, see ["Changing the Password for NSS DB" on page 165](#).

- **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`
- **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

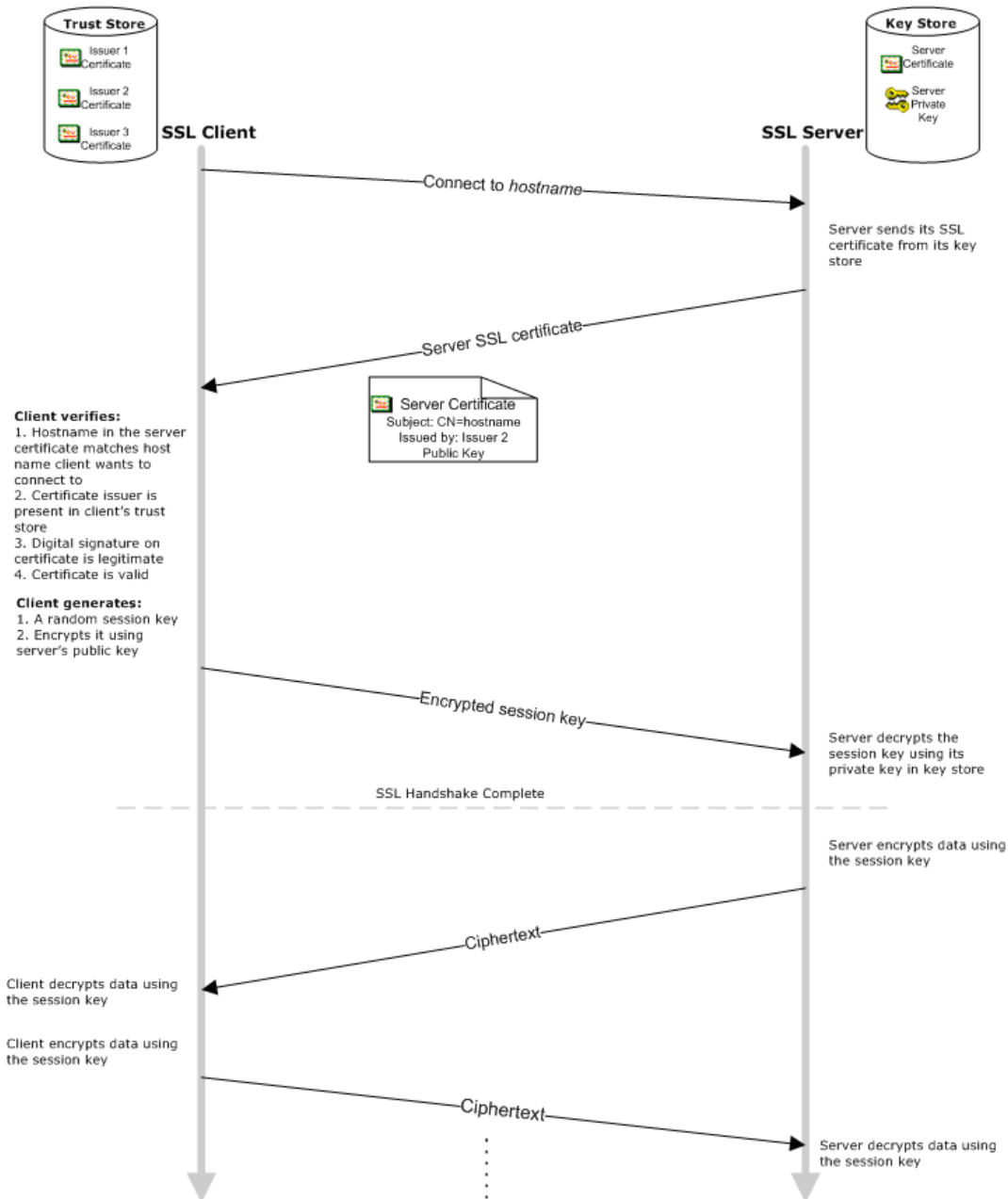
When a client initiates communication with the SSL server, the server sends its certificate to authenticate itself to the client. The client validates the certificate by verifying:

- 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 (applicable to default mode only)
- Demo (applicable to default mode only)

CA-signed certificates are issued by a third party you trust. The third party may be a commercial Certificate Authority (CA) such as VeriSign and Thawte or you might have designated your own CA. Because you trust this third party, your client's 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 `keytool` (runs from the command line in a terminal window) and `keytoolgui` (provides a graphical user interface) commands enable you to perform SSL configuration tasks. The preferred tool is `keytool`, which does not require the X Window system.

Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred on the Manager machine, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Using `keytoolgui` on Console machines is fine, but be aware that `keytoolgui` does not work on the Mac, so for managing the keystore and certificates and so on, on a Mac, use `keytool`.

HP's `keytool` simplifies usage of JRE `keytool` by pre-populating several command line arguments of JRE `keytool` command based on component's configured values. These command line arguments include: `-keystore`, `-storepass`, and `-storetype` (with exceptions that will be discussed in later sections in the context of certain commands). The following sections present `keytool` command lines that are exactly formed to perform the task mentioned in the section. Use only those options to perform the documented tasks. Note that if you use `keytool -h` to view Help you will see options that are not

covered in this documentation. The `keytool` examples presented in this guide do not display all possible `keytool` options.

For details on `keytool` in general, see online vendor documentation. Various vendors have their own version of `keytool`. One reference is <http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>.

Export a Key Pair

You can use `keytool` to export a key pair. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Exporting a Key Pair Using `keytool`

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need. Note that this command does not use the HP `keytool` wrapper and requires more options be specified than some other `keytool` commands.

To export key pair with the alias `testkey` into a file named `config/jetty/keystore.p12` from `keystore config/jetty/keystore`:

```
<ARCSIGHT_HOME>/jre/bin/keytool -importkeystore -srckeystore config/jetty/keystore  
-srcstoretype JKS -destkeystore config/jetty/keystore.p12 -deststoretype PKCS12 -  
srcalias testkey
```

Exporting a Key Pair Using `keytoolgui`

To use `keytoolgui`:

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 46](#).
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 46](#).

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

You can use `keytool` to import a key pair. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Importing a Key Pair Using `keytool`

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need. Note that this command does not use the HP `keytool` wrapper and requires more options be specified than some other `keytool` commands.

To export key pair with the alias `testkey` from a file named `config/jetty/keystore.p12` into the file `config/jetty/keystore.new`:

```
<ARCSIGHT_HOME>/jre/bin/keytool -importkeystore -srckeystore  
config/jetty/keystore.p12 -srcstoretype PKCS12 -destkeystore  
config/jetty/keystore.new -deststoretype jks -srcaias testkey
```

Importing a Key Pair Using `keytoolgui`

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 46](#).
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 46](#).

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

You can use `keytool` to export a certificate. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Exporting a Certificate Using `keytool`

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need.

Note that if the alias points to a trusted certificate, the output is that certificate. Also, if the alias points to a key entry, the output is the first certificate from key's certificate chain.

For example:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -exportcert -store managerkeys -alias testkey  
-file /tmp/testkey.cer
```

Exporting a Certificate Using `keytoolgui`

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 45](#).
4. Right-click the certificate and select **Export**.

- a. Select **Head Certificate** as Export Type and **DER Encoded** as the Export Format 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 **Export Successful** 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

You can use `keytool` to import a certificate. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Importing a Certificate Using `keytool`

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need.

In this example, the command imports a certificate from the specified file into manager keystore and it sets the alias `<testkey>` to that certificate. Specify passwords for your keystore when needed. Note that if the keystore contains a key with specified alias, then `keytool` assumes that you are importing a certificate reply from CA. If there is no a key with such an alias in the keystore, then `keytool` imports a trusted certificate for that alias.

For example:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -importcert -store managerkeys -alias testkey  
-file /tmp/tms_root.cer
```

Importing a Certificate Using `keytoolgui`

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

```
./arcsight keytoolgui
```

2. Click **File->Open keystore** and navigate to 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 45.
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 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.

Click **OK**.

8. The Certificate details are displayed. Click **OK**.
9. You see the message **Do you want to accept the certificate as trusted?**. 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 (for example *devgroup.topco.com*).

11. You see the message **Trusted Certificate Import Successful..** Click **OK**.
12. Save the truststore file.

Creating a Keystore

You can use `keytool` or `keytoolgui` to create a keystore. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Creating a Keystore Using keytool

An example of a `keytool` command line is provided below. Use this example as a basis to form the command line you need. Note that this command does not use the HP `keytool` wrapper and requires more options be specified than some other `keytool` commands.

The abbreviations in the command below denote the following fields: `cn` = Common Name, `ou` = Organizational Unit, `o` = Organization, and `c` = Country.

The command generates a new self-signed certificate with `ALIAS_NAME` in the specified keystore `PATH_TO_KEYSTORE`.

Example for a new keystore:

```
<ARCSIGHT_HOME>/jre/bin/keytool -genkeypair -keystore config\keystore.client -  
storetype JKS -storepass password -dname "cn=John Smith, ou=ArcSight, o=HP, c=US" -  
alias testKey -validity 365
```

Specify all the options in the above example using the appropriate values for your installation.

As a separate operation, either before or after you run the `genkeypair` command, you have to set the values for the keystore location, keystore type, and password in the `client.properties` file. This file is in `<ARCSIGHT_HOME>/config` (for example, `C:\arcsight\Console\current\config`). The Console uses this file to access the keystore during authentication.

The `client.properties` file works as an override for the `client.defaults.properties` file. (You do not edit the default properties file because it is overwritten at upgrade time.) Set these properties in `client.properties`, as follows:

- **ssl.keystore.path**= Set this value if it differs from the default in `client.defaults.properties`. It must be the same as the path specified in the `-keystore` option in the command example, above.
- **ssl.keystore.type**= Set this value if it differs from the default in `client.defaults.properties`. It must be the same as the path specified in the `-storetype` option in the command example, above.
- **ssl.keystore.password**=Set this value if it differs from the default in `client.defaults.properties`. It must be the same as the password specified in the `-storepass` option in the command example, above. The default is blank (no password), but having a password is recommended.

However, if you plan to encrypt the password (also recommended), there is no need to set it manually in this file. You specify it and encrypt it using the `changepassword` command, next.

To set an encrypted password, run the following command:

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

This command prompts you for the actual password, adds it to the `client.properties` file, and encrypts it. It must be the same as the password specified in the `-storepass` option in the command example, above.

Creating a Keystore Using keytoolgui

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

```
./arcsight keytoolgui
```

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

Generating a Key Pair

You can use `keytool` to generate a key pair. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Generating a Key Pair Using `keytool`

The abbreviations in the command below denote the following fields: `cn` = Common Name, `ou` = Organizational Unit, `o` = Organization, and `c` = Country.

For example:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -genkeypair -store managerkeys -dname "cn=John Smith, ou=ArcSight, o=HP, c=US" -alias testKey -validity 365
```

Provide a key password for `<testKey>`, or press Enter using same as password as the keystore password).

Generating a Key Pair Using `keytoolgui`

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

```
./arcsight keytoolgui
```

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

View Certificate Details From the Store

You can use `keytool` to view certificate details from the keystore (list the entries in a keystore). Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Viewing a Certificate Details from the Store Using keytool

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need. Note that this command does not use the HP `keytool` wrapper and requires more options be specified than some other `keytool` commands.

To list all existing keys:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -store managerkeys -list
```

To print details for the key with the specified alias:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -store managerkeys -list -alias mykey -v
```

Viewing a Certificate Details from the Store Using keytoolgui

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 45](#).
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` or `nssdb.client`, use the `runcertutil` command to view certificate information. See ["runcertutil" on page 123](#), for more information.

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

Delete a Certificate

You can use `keytool` to delete a certificate from the keystore. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Deleting a Certificate Using keytool

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need. Note that this command does not use the HP `keytool` wrapper and requires more

options be specified that some other `keytool` commands.

To remove the ESM certificate `mykey`:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -store managerkeys -delete -alias myKey
```

To remove a third party trusted certificate with alias `rootCA`:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -store managercerts -delete -alias rootCA
```

Deleting a Certificate Using `keytoolgui`

To delete a certificate from the truststore, start `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:

Note: 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 will use it to open the keystore.
- e. Continue 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 54](#).

Note: 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. Run the following command to do so:

```
/etc/init.d/arcsight_services restart manager
```
6. Restart all clients.
7. When installing a new client, repeat Steps 2-4 of this procedure.
8. Optionally, if SSL client-side authentication is needed, on the ArcSight Console, perform the steps listed in section ["Setting up SSL Client-Side Authentication on ArcSight Console " on page 70](#)

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 of the procedure ["When Clients Communicate With One Manager" on page 59](#) 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 `keytool` or `keytoolgui` command to import certificates into the truststore (`cacerts`):

The `keytool` command is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance. See ["Import a Certificate" on page 54](#) for details on using `keytool`.

To use the `keytoolgui` command:

- 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 47](#).
- d. Click **Tools->Import Trusted Certificate**:
 - i. Select the self-signed certificate for a Manager and click **Import**.
 - ii. You see the 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.

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 message **Trusted Certificate Import Successful..** 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 a certificate signed by a Certificate Authority means replacing your demo or self-signed certificate. Follow the procedures described in this section to obtain and import the certificate into the Manager.

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

- 1. ["Create a Key Pair for a CA-Signed Certificate" below.](#)
- 2. ["Send for the CA-Signed Certificate" on the next page.](#)
- 3. ["Import the CA Root Certificate" on page 64.](#)
- 4. ["Import the CA-Signed Certificate" on page 65.](#)
- 5. ["Restart the Manager" on page 68.](#)
- 6. ["Accommodating Additional Components" on page 68.](#)
- 7. Optionally, if SSL client-side authentication is needed, on the ArcSight Console, perform the steps listed in section ["Setting up SSL Client-Side Authentication on ArcSight Console" on page 70](#)

Create a Key Pair for a CA-Signed Certificate

To create a key pair, the `keytool` command is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window

system is not present on the ESM Express appliance. See ["Generating a Key Pair" on page 57](#) for details on using `keytool`.

To use the `keytoolgui` command:

1. On the Manager machine, run this command to launch `keytoolgui` 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`.

Send for the CA-Signed Certificate

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

You can use `keytool` to send for a CA-signed certificate. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

Sending a CA-Signed Certificate Using `keytool`

An example of a `keytool` command line is provided. Use this example as a basis to form the command line you need.

For example:

```
<ARCSIGHT_HOME>/bin/arcsight keytool -certreq -store managerkeys -alias testkey -  
file config/testkey.csr
```

The command creates signing request using the PKCS#10 format for a certificate with alias <ALIAS_NAME> from keystore_path. Here <storepass> is keystore password, and <keypass> is a password for the specified alias. No need to be specified for empty values. As a result the command creates a file <request.csr> that should be sent to 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 (cer-file).

Sending a CA-Signed Certificate Using keytoolgui

1. In `keytoolgui`, 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.

To create a key pair, the `keytool` command is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance. See ["Import a Certificate" on page 54](#) for details on using `keytool`.

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 `keytoolgui` 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 47](#).
 - 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: Hints on importing the CA root certificate:

- 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 of the procedure on one of the Consoles.
 - Copy the updated cacerts to any Logger, 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-----
MIICjTCCAfaGAWIBAgIDWnWvMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQTEiMCAGA1UECBMZrk9
SIFRFU1RJTkcgUFVFSUE9TRVMgT05MWTEDMBsGA1UEChMUUVGhhd3R1IEN1cnRpZm1jYXRpb24xZzAVBgNVBA
sTD1RFU1QgVEVTVCBURVNUMRwwGgYDVQQDExNUaGF3dGUgVGZzdCBDQSBSb290MB4XDTAyMDkyNzIzMzI0M
VoXDTAyMTAxODIzMzI0MVowADELMAkGA1UEBhMCrVMxDTALBgNVBAgTBGJ3YWgxDALBgNVBAcTBGJ3YWgX
DTALBgNVBAoTBGJ3YWgxDALBgNVBAcTBGJ3YWgXDTALBgNVBAMTFHppZXIuc3YuYXJjc2lnaHQy29tMIG
fMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b+BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vw
N4JVic
CSBkDpiqVF7K11Sx4ZVSXX4+VQ6k4gT5G0kDNvQeN05wwkzEMygMB+ZBnYqPA/XtWRZtjxvH
MoqS+JEqHruimLITC6q0reUB/txby6+S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHSUEDDAKBggrBgEFBQC
DATAMBgNVHRMBAg8EAjAAMA0GCSqGSIb3DQEBAUAA4GBAFY37E60+P4b3zTLNaG7EVM57GtKED6PwCIi1B
6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQVQxnpABjzTa1RfYgjNFJ61tI6ZKjB05kim9UBeCnKiNNzhIyDyFw
bHXOPB/JaLIV+jGugYNS7hf/ay0BXXK1fue007EgjhB/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.
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**) you saved in Step 7 of "[Create a Key Pair for a CA-Signed Certificate](#)" on page 62. 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 of "[Create a Key Pair for a CA-Signed Certificate](#)" on page 62.
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, `keytoolgui` 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.
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 saved as `keystore.old`.
11. Copy <ARCSIGHT_HOME>/config/jetty/keystore.request to <ARCSIGHT_HOME>/config/jetty/keystore.
12. For successful reconfiguration and Manager startup, enter the keystore passwords into the

appropriate properties file.

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 the next page](#).

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

Note: Also perform these steps on the Manager to update the Manager's cacerts so that Manager clients such as the `archive` command 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 64](#).)
- b. For one client, use `keytoolgui` 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 47](#).
 - iv. Click **Tools->Import Trusted Certificate** and select the certificate you copied earlier in this procedure.
 - v. You see the 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.

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.

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 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 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.

To delete an expired certificate, the `keytool` command is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance. To replace an expired certificate, you must delete the current certificate and import a new one. See ["Delete a Certificate" on page 58](#) and ["Import a Certificate" on page 54](#) for details on using `keytool`.

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 59](#), 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

This section describes the required steps for enabling client-authentication for ArcSight Console.

All communications between ESM and Console are performed over SSL connections. Which protocols and cipher suites to use for SSL connection is decided in the very beginning, during the initial SSL handshake. SSL handshake always validates that server could be trusted by reviewing and challenging its certificate. Optionally SSL handshake could validate client's certificate to ensure that connection was requested from a legitimate client. For that purpose the client provides SSL certificate and SSL handshake verifies that the client owns the corresponding private key.

Depending on the selected authentication mode the described below configuration steps might have effect on overall user authentication. These are the implications of the various modes:

1. **Password Based Authentication:** No impact
2. **Password Based and SSL Client Based Authentication:** In this mode, the client sends the SSL certificate and password-based credentials. Both of them should identify exactly the same user.
3. **Password Based or SSL Client Based Authentication:** In this mode, the result depends on your choice. For this authentication mode Console's login dialog provides two buttons: "Login" and "SSL Client Login" to send either the username and password or the SSL certificate.
4. **SSL Client Only Authentication:** In this mode, authentication is performed based on SSL certificate only.

Unless it's PKCS#11 login in the modes 2 and 4 described above with configured client-side authentication, SSL Login will always be performed under the same user, because the login dialog will always use the same client certificate.

For PKCS#11 logins the authentication process uses the certificates from PKCS#11 token, so the result will depend on the provided token.

Regardless of PKCS#11 mode, SSL login authentication is performed on server-side in two steps by validating SSL certificate and then by looking up the ArcSight user with the external ID that matches CN (Common Name) from the provided certificate.

Note: Client-side authentication could be helpful when you want to establish connection from a client to ESM always under the same user account. That eliminates the need to provide username/password. If it's what you need use the following instructions and once the client certificate is created, select "SSL Client Only Authentication" mode for that client, and create ArcSight User (in ESM) with externalID matching CN from client certificate. Do not forget to secure access to this certificate. If keystore with the certificate is stolen, it could be used to access ESM from other clients.

Setting up SSL Client-Side Authentication on ArcSight Console

You can use `keytool` to import a certificate. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

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 `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 Generate Certificate dialog.
- e. Enter an alias for the key pair and click **OK**:

Caution: If you plan to install the Console and Manager on the same machine, make sure that this alias is unique. Also, do not use the machine name or IP address for the alias.

- f. Enter a password for the keystore and confirm it and click **OK**.
2. Save the keystore in the Console's <ARCSIGHT_HOME>/config directory by clicking **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.
Example keytool command line:

```
jre/bin/keytool -genkeypair -keystore config/keystore.client -storetype JKS  
-storepass password -dname "cn=John Smith, ou=ArcSight, o=HP, c=US" -alias  
testKey -validity 365
```

3. 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
```

Note: HP recommends encrypting the password in the property file to protect the password. If you decide to do then you don't need to enter the property "ssl.keystore.password" as it's described above, but you can simply run the `changepassword` tool to set an encrypted keystore password in the `client.properties` file: `arcsight changepassword -f config/client.properties -p ssl.keystore.password`

You will be asked to enter the value for the specified unencrypted property and the command will automatically add the new property `ssl.keystore.password.encrypted` for you. During that call the unencrypted property is removed.

4. If you are using a self-signed certificate, skip to step 7. Otherwise, create a Signing Request by following the steps in ["Send for the CA-Signed Certificate" on page 63](#) and ["Import the CA-Signed Certificate" on page 65](#).
Send a request to the certificate authorities and import the signed certificate into the Console's **keystore**. Example for keytool command line:

```
bin/arcsight keytool -certreq -store clientkeys -alias testkey -file  
config/testkey.csr..
```

5. After receiving a response, follow the steps in "[Import the CA Root Certificate](#)" on page 64. Import the CA Root Certificate into the Console's **truststore**. Example for `keytool` command line:

```
bin/arcsight keytool -importcert -store clientkeys -alias testkey -file  
/tmp/signed-cert.cer
```

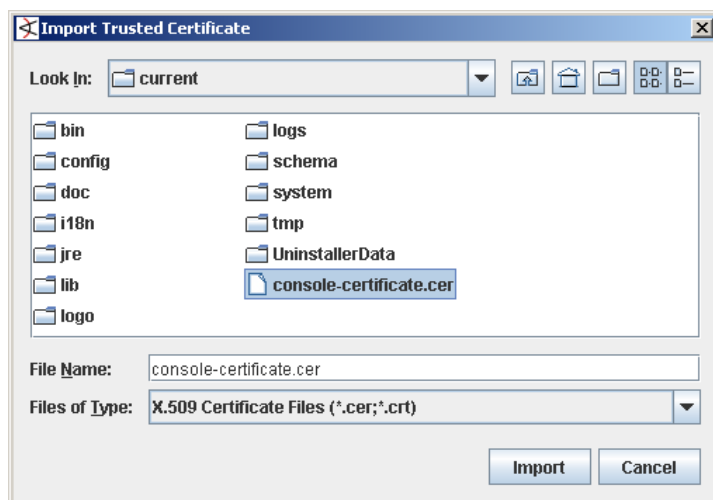
6. Export the client's certificate into `cer`-file:
 - a. In `keytoolgui`, right-click the key pair you just generated and select **Export**.
 - b. Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format and click **OK**.
 - c. Enter a name for the certificate with a `.cer` extension and click **Export**.
 - d. You see the **Export Successful** message.
 - e. If your Console is on a different machine than the Manager, copy this certificate to the Manager's machine. Example for `keytool` command line:

```
bin/arcsight keytool -exportcert -store clientkeys -alias testkey -file /tmp/console-certificate.cer
```

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 `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 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 may confirm whether or not you trust the certificate.

Click **OK**.

- g. Review the certificate details and click **OK**.
- h. In response to **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 ESM truststore. ESM reads its truststore during start up, so you need to restart ESM in order to enable newly imported certificates. Example for keytool command line:

```
bin/arcsight keytool -importcert -store managercerts -alias testkey -file  
/tmp/console-certificate.cer
```

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.

Setting Up Client-Side Authentication for ACC

You can use `keytool` to import a certificate. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

To set up client-side authentication for ACC, you must export the Console's private key into a p12-file, and then import that file into the browser's internal truststore.

1. Export the Console's private key:
 - a. From the Console's <ARCSIGHT_HOME>/bin directory start `keytoolgui` by running the following command:

```
./arcsight keytoolgui
```
 - b. Click **File > Open keystore** and navigate to the Console keystore you created.
 - c. Right-click on the Console's keypair and select **Export**.
 - d. Select **Private Key and Certificates** as the **Export Type** and **PKCS#12** as the **Export Format** (if not already selected). Click **OK**.
 - e. Enter the password for that you have set for the Console's keystore when prompted and **OK**.
 - f. Enter a new password for the keystore and confirm the password. 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 `keytoolgui`.

Example `keytool` command line:

```
keytool -importkeystore -srckeystore config\keystore.client -srcstoretype jks  
-srcstorepass password -destkeystore config/consolekey.p12 -deststoretype  
PKCS12 -srcalias testconsolekey
```

The above command creates a new file `config/consolekey.p12` with keystore of the type **PKCS12** and stores there a private key for alias **testconsolekey** from client's keystore file `config/keystore.client`.

2. Use keystore `config/consolekey.p12` that contains Console's private key to export the certificate into internal browser's keystore:
 - On Firefox: Select **Tools > Options > Advanced > View Certificates > Your Certificates/Import**. Then specify file, submit, and restart the browser.

- On Internet Explorer and Chrome: Select **Control Panel > Internet Options > Content > Certificates > Personal > Import**. Then specify file, submit, and restart the browser.

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 52](#) for details.)
 - a. In `keytoolgui`, click **Tools->Generate Key Pair**.

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

- 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.

Example command for `keytool` command line:

```
jre/bin/keytool -genkeypair -keystore config/keystore.client -storetype JKS -  
storepass password -dname "cn=John Smith, ou=ArcSight, o=HP, c=US" -alias  
testKey -validity 365
```

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>
```

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

4. Export the client's (Connector) certificate using `keytoolgui`. See section ["Export a Certificate" on page 53](#) for details.

Example command for `keytool` command line:

```
bin/arcsight keytool -exportcert -store clientkeys -alias testkey -file  
/tmp/agent-certificate.cer
```

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`.

Example command for `keytool` command line:

```
bin/arcsight keytool -importcert -store managercerts -alias testkey -file  
/tmp/agent-certificate.cer
```

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, and SmartConnectors.

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 59.
2. Follow the instructions in "[Verifying SSL Certificate Use](#)" below 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](#)" below 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](#)" below 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, 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 accepts login calls with empty passwords and use the Subject CN (Common Name) from the user's certificate to identify the user.

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.

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

To configure the or 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, verify that:

- 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. Log 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.

Chapter 4: Running the Manager Configuration Wizard

After you have installed and configured your system, you can change some configuration parameters by running the `managersetup -i console` command in a terminal window to launch the Manager Configuration Wizard. Running the command in console mode is the preferred way of launching the wizard. Using the X Window system to run the wizard in graphical user interface mode is not preferred, but if you have the X Window system installed and want to use it, you can run the `managersetup` command without options to launch the wizard. The X Window system is not present on the ESM Express appliance.

If issues occur while running the Manager Configuration Wizard, this command logs troubleshooting information in a log file: `/opt/arcsight/manager/logs/default/serverwizard.log`.

Running the Wizard

Run the wizard as user *arcsight*. Before you run the Manager Configuration 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 -i console
```

Note: If you want to install X Window to use the GUI mode you can get the following error if X Window is not set up correctly:

Could not initialize class sun.awt.X11GraphicsEnvironment.

To fix it, ensure that your X Window system is set up properly and try again.

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

1. Select either **Run manager in default mode** or **Run manager in FIPS mode**. For information on FIPS, see ["Configuration Changes Related to FIPS " on page 155](#)
2. You can enter **Manager Host Name**, **Manager Port**, and **Physical Location**. To change the hostname or IP address for your Manager host, enter the new one. The Manager host name that you enter appears on the Manager certificate. If you change the host name, be sure to regenerate the Manager's certificate in by selecting Replace with the new Self-Signed key pair in the screen that allows you to select key pair options (make a note of this if you change your host name). We recommend that you do not change the Manager Port number.
3. 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**.

If you selected **Replace the current license file**, you are prompted for the new one.

4. Select the Java Heap memory size. 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.)
5. Now select a key pair option. 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 the first or second step above, 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.

6. Accept the **Logger JDBC URL** and **Database Password** defaults.
7. Select the desired authentication method (password based or SSL client only).
8. Select the method for authenticating the users. See ["Authentication Details" on the next page](#) for more details on each of these options.
9. Accept the default (**Internal SMTP server**) 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 options are requested, 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.
10. The Manager can automatically create an asset when it receives an event with a new sensor or device information. The default, **Enable Sensor Asset Creation**, ensures that assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation**.

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.

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.

After 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.

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	<p>Host name of the RADIUS server.</p> <p>To specify multiple RADIUS servers for failover, enter comma-separated names of those servers in this field.</p> <p>For example, server1, server2, server3. If server1 is unavailable, server2 is contacted, and if server2 is also unavailable, server3 is contacted.</p>

Parameter	Description
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.

Parameter	Description
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` command.

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` command.

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.

Note: 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.

For more detail on SSL authentication for browser logins, see "Login in with SSL Authentication" in the chapter "Starting the Command Center" in the ArcSight Command Center Guide.

SSL Client Only Authentication

You must manually set up the authentication of the client certificate by the Manager. You can either use a PKCS#11 Token or a client keystore to authenticate.

Appendix A: Administrative Commands

This appendix provides information about assorted administrative commands.

ArcSight_Services Command

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

Note: Do not start or stop services that are listed in the category Background Component Services. They are listed for information only.

Description	This command manages component services.	
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.
	<code>stop</code>	Stop the specified component and any components that depend on it.
	<code>restart</code>	Complete a controlled stop and restart of the specified component service and any component it depends on. 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.
Component Services	<code>all</code>	This is the default if no component is specified.
	<code>logger_httpd</code> <code>logger_servers</code> <code>logger_web</code> <code>manager</code> <code>mysqld</code>	Logger Apache httpd service Logger service Logger Web service ESM Manager MySQL database

Background Component Services (for information only)	aps	ArcSight Platform Services; functions in background to perform configuration tasks; you can start this service, but do not stop it unless you are stopping all services
	postgresql	Open source database, which functions in the background; you can start this service, but do not stop it unless you are stopping all services
	execprocsvc	Helper service for the Manager; actions not supported on this service
Examples	<pre>/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</pre>	

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 (on Windows) or 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	This command generates a report on ACLs either at the group level or at the user level. By default, the generated report is placed in the /opt/arcsight/manager/ACLReports directory.	
Applies to	Manager	
Syntax	ACLReportGen [parameters]	
Parameters	Optional:	

ACLReportGen, continued

	-config <config>	The primary configuration file (config/server.defaults.properties).
	-locale	The locale under which to run the command.
	-mode <mode>	Mode in which this tool is run to generate the ACLs report. Supported modes are <code>grouplevel</code> and <code>userlevel</code> . The default value is <code>grouplevel</code> .
	-pc <privateConfig>	The name of the override configuration file (config/server.properties).
	-h	Help
Example	arcsight ACLReportGen	

agent tempca

Description	This command allows you to inspect and manage temporary certificates for a SmartConnector host machine	
Applies to	SmartConnectors	
Syntax	agent tempca	
Parameters		For parameters, see the description of the tempca command for the Manager.
Example	arcsight agent tempca	

agentcommand

Description	This command allows you to send a command to SmartConnectors	
Applies to	SmartConnectors	
Syntax	agentcommand -c (restart status terminate)	
Parameters	-c	Valid parameters are <code>restart</code> , <code>status</code> , or <code>terminate</code> .

agentcommand, continued

Examples	<p>To retrieve status properties from the SmartConnector:</p> <pre>arcsight agentcommand -c status</pre> <p>To terminate the SmartConnectorprocess:</p> <pre>arcsight agentcommand -c terminate</pre> <p>To restart the SmartConnectorprocess:</p> <pre>arcsight agentcommand -c restart</pre>
----------	--

agents

Description	This command runs all installed ArcSight SmartConnector on the host as a standalone application.	
Applies to	SmartConnectors	
Syntax	agents	
Parameters	None	
Example	arcsight agents	

agentsvc

Description	This command installs an ArcSight SmartConnector as a service.	
Applies to	SmartConnectors	
Syntax	agentsvc -i -u <user>	
Parameters	-i	Install the service.
	-u <user>	Run service as specified user.
Example	arcsight agentsvc	

agentup

Description	This command allows you to verify the current state of a SmartConnector. It returns 0 if the SmartConnector is running and accessible, and returns 1 if it is not.	
Applies to	SmartConnectors	
Syntax	agentup	
Parameters	None	
Example	arcsight agentup	

arcdt

Description	This command allows you to run diagnostic utilities such as session wait times, and thread dumps about your system, which can help Customer Support analyze performance issues on your components.	
Applies to	Manager	
Syntax	arcdt diagnostic_utility utility_Parameters	
Parameters	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 command.</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 or 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>

arcdt, continued

		<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 StartTime or mrt, value is like yyyy-MM-dd-HH-mm-ss-SSS-zzz; if type is EventId, value is a positive integer indicating the start 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>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>

arcdt, continued

		<p>thread-dumps—Obtain thread dumps from the Manager. Optional parameters which can be specified</p> <p>-c <count>— The number of thread dumps to request. (3)</p> <p>-f <frequency> —The interval in SECONDS between each thread dump request. (10)</p> <p>-od <outputdir>— The output directory into which the requested thread dumps have to be placed. ()</p>
	<p>help</p> <p>help commands</p> <p>help <command></p>	<p>Use these help Parameters (no dash) to see the Parameters, a list of commands, or help for a specific command.</p>
Examples	<p>To find out the number of cases in your database:</p> <ol style="list-style-type: none"> 1. Create a file called <code>sample.txt</code> in <code><ARCSIGHT_HOME>/temp</code> on the Manager with this SQL command: <pre>select count(*) from arc_resource where resource_type=7;</pre> 2. Run this command in <code><ARCSIGHT_HOME>/bin</code>: <pre>arcsight arcdt runsql -f temp/sample.txt</pre> 	

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>
```

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

archive

Description	This command imports or exports resources (users, rules, and so on) to or from one or more XML files. 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	archive -f <archivefile> [Parameters]	
Required Parameter	-f <archivefile>	The input (import) or the output (export) file specification. File name paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME>, not the current directory.
Optional Parameters	-action <action>	Possible actions include: diff, export, i18nsync, import, list, merge, sort, and upgrade. Default: export.
	-all	Export all resources in the system (not including events).
	-autorepair	Check ARL for expressions that operate directly on resource URI's.
	-base <basefile>	The basefile when creating a migration archive. The new archive file is specified with -source (the result file is specified with -f).
	-config <file>	Configuration file to use. Default: config/server.defaults.properties
	-conflict <conflictpolicy>	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.

archive, continued

	-exportaction <exportaction>	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.
	-format <fmt>	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.
	-h	Get help for this command.
	-i	(Synonym for -action import.)
	-m <manager>	The Manager to communicate with.
	-o	Overwrite any existing files.
	-p <password>	Password with which to log in to the Manager.
	-param <archiveparamsfile>	The source file for parameters used for archiving. Any parameters in the named file can be overridden by command line values.
	-pc <configfile>	Private configuration file to override -config. Default: config/server.properties
	-pkcs11	Use this option when authenticating with a PKCS#11 provider. For example, arcsight archive -m <hostname> -pkcs11 -f <file path>
	-port <port>	The port to use for Manager communication. Default: 8443
	-q	Quiet: do not output progress information while archiving

archive, continued

	-source <sourcefile>	The source file. This is used for all commands that use the -f to specify an output file and use a separate file as the input.
	-standalone	Operate directly on the Database, not the Manager. Warning: Do not run archive in -standalone mode when the Manager is running; database corruption could result.
	-u <username>	The user name to log in to the Manager
	-uri <includeURIs>	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 "/All Filters/Geographic/West Coast") with a space, or repeat the -uri switch
	-urichildren <includeURIchildren>	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.
	-xrefids	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.
	-xtype <excludeTypes>	The types to exclude during export. No effect during import. Exclude types must be valid type names, such as Group, Asset, or ActiveChannel.
	-xtyperef <excludeTypeRefs>	The types to exclude during export (there is no effect during import). This is the same as -xtype, except it also excludes all references of the given type. These must include only valid type names such as Group, Asset, and ActiveChannel.
	-xuri <excludeURIs>	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.

archive, continued

	<p>-xurichildren <excludeURIchildren></p> <p>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.</p>
Examples	<p>To import resources from an XML file (on a Unix host):</p> <pre>arcsight archive -action import -f /user/subdir/resfile.xml</pre> <p>To export certain resources (the program displays available resources):</p> <pre>arcsight archive -f resfile.xml -u admin -m mgrName -p pwd</pre> <p>To export all resources to an XML file in quiet, batch mode:</p> <pre>arcsight archive -all -q -f resfile.xml -u admin -m mgrName -p password</pre> <p>To export a specific resource:</p> <pre>arcsight archive -uri "/All Filters/Geographic/West Coast" -f resfile.xml</pre> <p>Manual import (program prompts for password):</p> <pre>arcsight archive -i -format preferarchive -f resfile.xml -u admin -m mgrName</pre> <p>Scheduled or batch importing:</p> <pre>arcsight archive -i -q -format preferarchive -f resfile.xml -u admin -m mgrName -p password</pre> <p>Scheduled or batch exporting:</p> <pre>arcsight archive -f resfile.xml -u admin -m mgrName -p password uri "/All Filters/Geographic/East Coast" -uri "/All Filters/Geographic/South"</pre>

Make sure that the archive tool client can trust the Manager's SSL certificate. See ["SSL Authentication" on page 44](#) for information on managing certificates.

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

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.

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

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

Note: 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 "[SSL Authentication](#)" on page 44 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.

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 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 "[SSL Authentication](#)" on page 44, 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	This command changes the contents of the archive. The <code>archivefilter</code> command takes a source archive xml file as input, applies the filter specified and writes the output to the target file.
-------------	---

archivefilter, continued

Applies to	Manager	
Syntax	archivefilter -source <sourcefile> -f <archivefile > [Parameters]	
Parameters	-a <action>	Action to perform can be insert, or remove}. if you specify nothing, no action is performed.
	-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

archivefilter, continued

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

bleep

Description	<p>This command is an unsupported stress test to supply a Manager with security events from replay files (see <code>replayfilegen</code>). Replay files containing more than 30,000 events require a lot of memory on the bleep host.</p> <p>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.</p> <p>Run <code>arcsight tempca -ac</code> on the bleep host if the Manager under test is using a demo certificate.</p> <p>Create the file <code>config/bleep.properties</code> using the descriptions in <code>bleep.defaults.properties</code>.</p>	
Applies to	Manager	
Syntax	bleep [-c <file>] [-D <key>=<value> [<key>=<value>...]]	
Parameters	-c file	Alternate configuration file (default: <code>config/bleep.properties</code>)
	-D <key>=<value>	Override definition of configuration properties
	-m <n>	Maximum number of events to send. (Default: -1)

bleep, continued

	-n <host>	Manager host name
	-p <password>	Manager password
	-t <port>	Manager port (Default: 8443)
	-u <username>	Manager user name
	-h	Help
Examples	To run: arcsight bleep	

bleepsetup

Description	This command runs a wizard to create the bleep.properties file.	
Applies to	Manager	
Syntax	bleepsetup	
Parameters	-f	Properties file (silent mode)
	-i	Mode: {swing, console, recorderui, silent} Default: swing
	-g	Generate sample properties file
Examples	To run: arcsight bleepsetup	

changepassword

Description	This command changes obfuscated passwords in properties files. The utility prompts for the new password at the command line.	
Applies to	Manager	
Syntax	changepassword -f <file> -p <property_name>	
Parameters	-f <file>	Properties file, such as config/server.properties
	-p <property_name>	Password property to change, such as server.privatekey.password
Examples	To run: arcsight changepassword	

checklist

Description	<p>This command is the ArcSight Environment Check. Used internally by the installer to see if you have the correct JRE and a supported operating system.</p> <p>This can run from the Manager.</p>
-------------	--

console

Description	This command runs the ArcSight Console.	
Applies to	Console	
Syntax	console [-i] [parameters]	
Parameters	-ast <file>	
	-debug	
	-i	
	-imageeditor	
	-laf <style>	<p>Look and feel style: metal, plastic, plastic3d.</p> <p>The default style is plastic3d.</p>
	-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	<p>To run the console:</p> <p>ArcSight Console</p>	

consolesetup

Description	This command runs 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	This command runs the 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	This command allows you to 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.

exceptions, continued

	-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	This command exports your database tables. On completion, the command generates two files: a temporary parameter file and the actual database dump file, which is placed in /opt/arcsight/manager/tmp.	
Applies to	Manager	
Syntax	export_system_tables <username> <password> <DBname>	
Parameters	<username>	CORR-Engine username
	<password>	Password for the CORR-Engine user
	<DBname>	Name of the CORR-Engine from which you are exporting the system tables
	-s	Include session list tables

export_system_tables, continued

Examples	<p>To run:</p> <pre>arcsight export_system_tables <DB username> <password> <DBname></pre> <p>Trend resources are exported, but not trend data from running them. After you import, re-run the trends to generate new data.</p>
----------	--

flexagentwizard

Description	This command generates simple ArcSight FlexConnectors.	
Applies to	SmartConnectors	
Syntax	flexagentwizard	
Parameters	None	
Examples	<p>To run:</p> <pre>arcsight flexagentwizard</pre>	

groupconflictingassets

Description	This command groups asset resources with common attribute values (the 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>	The protocol can be http or https. If you do not specify one, the default is https.
	-u <name>	User name

groupconflictingassets, continued

	-h	Help
Examples	To run: arcsight groupconflictingassets	

idefensesetup

Description	This command runs a wizard to configure iDefense appliance information on the Manager.	
Applies to	Manager	
Syntax	idefensesetup	
Parameters	-f <logfile name>	Optional properties file name (silent mode)
	-i <mode>	The mode can be 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	This command imports 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 CORR-Engine, and it is always arcsight.

import_system_tables, continued

	<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	<pre>arcsight import_system_tables dbuser mxyzptlk arcsight arcsight_dump_system_tables.sql</pre> <pre>import_system_tables dbuser mxyzptlk arcsight /home/root/arcsight_dump_system_tables.sql</pre> <p>Note: Trend resources are exported, but not trend data from running them. After you import, re-run the trends to generate new data.</p>	

keytool

Description	This command runs the Java Runtime Environment keytool utility to manage key stores.	
Applies to	Manager, Console, SmartConnectors	
Syntax	keytool -store <name>	
Parameters	-store <name>	<p>(Required) The specific store can be managerkeys, managercerts, clientkeys, clientcerts, ldapkeys, or ldapcerts.</p> <p>(original parameters) All parameters supported by the JRE keytool utility are passed along. Use arcsight keytool</p>
	-help	For a list of parameters and arguments. Also, use the command keytool without arguments or the arcsight prefix for more-detailed help.

keytool, continued

Examples	<p>To view Console key store:</p> <pre>arcsight keytool -store clientkeys</pre> <p>The parameters for this command are actually sub-commands and many of them have their own sub-commands or parameters. To see all the possible sub-commands use <code>-help</code> followed by the sub-command for which you want to see all sub sub commands or parameters.</p> <p>For example, if you have a keystore called "managecerts," you could type <code>keytool -help -store managecerts</code> to see a list of all 16 additional subcommands. Then you could run:</p> <pre>keytool -help -store managecerts -list</pre> <p>to get additional help with the sub sub-command <code>-list</code>.</p>
----------	---

keytoolgui

Description	<p>This command runs a graphical user interface command for manipulating key stores and certificates.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Note: Using <code>keytoolgui</code> requires that the X Window System be installed on your system. The X Window System is not present on the ESM Express appliance.</p> </div>	
Applies to	Manager, Console	
Syntax	<code>keytoolgui</code>	
Parameters	None	
Examples	<p>To run:</p> <pre>arcsight keytoolgui</pre>	

kickbleep

Description	This command runs a simple, standardized test using the bleep utility.	
Applies to	Manager	
Syntax	<code>kickbleep</code>	
Parameters	<code>-f</code>	Properties file (silent mode)
	<code>-g</code>	Generate sample properties file
	<code>-i</code>	Mode: {swing, console, recorderui, silent} Default: swing

kickbleep, continued

Examples	To run: arcsight kickbleep
----------	-----------------------------------

listsubjectdns

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

managerinventory

Description	This command displays 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

managerinventory, continued

	-h	Help
Examples	<p>To run:</p> <pre>arcsight managerinventory</pre>	

manager-reload-config

Description	This command loads 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	<p>To reload config:</p> <pre>arcsight manager-reload-config</pre> <p>To view the differences between the properties the Manager is currently using and the properties that this command loads:</p> <pre>arcsight manager-reload-config -diff</pre>	

managersetup

Description	<p>This command allows you to configure the manager by launching the Manager Configuration Wizard. You can launch the wizard in console mode by using the <code>-i console</code> option while running the command in a terminal window. Run it without any option to launch the wizard in the graphical user interface mode when you have the X Window system installed and wish to use it. For more information about using the wizard, see "Running the Manager Configuration Wizard" on page 80. The options are all optional.</p> <p>Note that using the X Window system (to run the Manager Configuration Wizard) is not preferred, but if you have it installed and want to use it, you do not have to use the <code>-i console</code> option. The X Window system is not present on the ESM Express appliance.</p> <p>If issues occur while running the Manager Configuration Wizard, this command logs troubleshooting information in a log file: <code>/opt/arcsight/manager/logs/default/serverwizard.log</code>.</p>	
Applies to	Manager	
Syntax	managersetup [options]	
Parameters	<code>-i <mode></code>	<p><code>console</code> -- you answer configuration questions in a terminal window. Use no other options. This is the preferred mode of operation, and the only mode available for the ESM Express appliance. Use the <code>-i console</code> mode if you get this error when you attempt to run in the Manager Configuration Wizard: <code>Could not initialize class sun.awt.X11GraphicsEnvironment</code>.</p> <p><code>swing</code> -- You answer the same questions in a graphical user interface. Use no other options.</p> <p><code>silent</code> -- Followed by the <code>-f</code> option, the configuration is read from a file that was created by the <code>recordui</code> mode or the <code>-g</code> option. Use no other options besides <code>-f</code>.</p> <p><code>recordui</code> -- You provide a file path and name and then answer questions in GUI mode while configuring this system. Your configuration is recorded in the specified file for use with the <code>silent</code> mode on some other system. Use no other options.</p> <p>Blank (no <code>-i</code> option at all) means Swing mode.</p>
	<code>-f <file></code>	The name of the file to use when running in <code>-i silent</code> mode.

managersetup, continued

	-g	Generate sample properties for <code>-i</code> silent mode. The sample properties are sent to <code>stdout</code> , but you can redirect this output to a file. If you edit the file to provide your own configuration information, you can use it as the file in the <code>-f</code> option in silent mode. Use no other options.
Examples	<p>To run:</p> <pre>arcsight managersetup -i console (runs in console mode)</pre> <pre>arcsight managersetup (runs in GUI mode)</pre> <pre>arcsight managersetup -g > /opt/mysetup.file(generate sample to edit)</pre> <pre>arcsight managersetup -i silent -f /opt/mysetup.file (configures system from file)</pre>	

managereadddump

Description	This command runs a 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>readddump</code> , doing so causes the Manager to restart. Specify this file when running <code>readddumps</code> , which provides a convenient HTML file with links to all the thread dumps in a summary format.	
Applies to	Manager	
Syntax	<code>managereadddump</code>	
Parameters	None	
Examples	<p>To run:</p> <pre>arcsight managereadddump</pre>	

managerup

Description	This command gets 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	

managerup, continued

Examples	To check that the Manager is up, running, and accessible: arcsight managerup
----------	---

monitor

Description	This command is used with the Network Management Systems.	
Applies to	Manager	
Syntax	monitor	
Parameters	-a <filter>	Attribute filter. Default: ""
	-append	Append to output file instead of overwriting (Default: false)
	-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 for management service information. Default is stdout
	-p <pwd>	Password
	-sanitize	Sanitize IP address and host names (Default: false)
	-u <name>	User name
Examples	To run: arcsight monitor	

netio

Description	This command is a 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

netio, continued

Examples	To run: arcsight netio
----------	-------------------------------

package

Description	<p>This command imports or exports resources (users, rules, and so on) to or from one or more XML files (.arb files).</p> <p>Use this command instead of the archive command.</p> <p>Note: Some functionality for this command are available from the GUI only.</p>	
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

package, continued

	-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

package, continued

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

portinfo

Description	This command runs a 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	This command re-enables a disabled user account.	
Applies to	Manager	
Syntax	reenableuser <username>	
Parameters	<username>	The name of the user resource to re-enable
Examples	To re-enable a disabled user: arcsight reenableruser <username>	

refcheck

Description	This command is a resource reference checker.	
Applies to	Manager	
Syntax	refcheck	
Parameters	None	
Examples	To run: arcsight refcheck	

regex

Description	This command is a graphical tool for regex-based FlexConnectors.	
Applies to	SmartConnectors	
Syntax	regex	

regex, continued

Parameters	None	
Examples	<p>To run:</p> <pre>arcsight regex</pre>	

replayfilegen

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

resetpwd

Description	<p>This command runs a wizard to reset a user's password and optionally notify the user of the new password by e-mail.</p>	
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

resetpwd, continued

	-h	Display command help
Examples	<p>To reset a user's password:</p> <pre>arcsight resetpwd</pre>	

resvalidate

Description	<p>This command checks for whether there are any invalid resources in the database. The utility generates two reports called <code>validationReport</code> (with <code>.xml</code> and <code>.html</code> 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.</p> <p>If you have more than 50,000 actors you should first increase your Java heap size to 8 GB before running this command.</p>	
Applies to	Manager, Database	
Syntax	<code>resvalidate</code>	
Parameters	<code>-excludeTypes <exclude_resource_names></code>	<p>Resource type to exclude from being checked; for example, Rule, DataMonitor</p> <p>If specifying multiple resource types to exclude, use comma to separate them.</p> <p>Resource type – Rule,DataMonitor (comma separated)</p>
	<code>-out <output_dir></code>	<p>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>
	<code>-persist [false true]</code>	<p>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.</p> <p>Default: <code>persist=true</code>.</p>

resvalidate, continued

Examples	<p>In general, if you need to run the resource validation script, run it twice: the first time with '-persist true' (default) to validate and fix invalid resources, and the second time with '-persist false' to generate a correct report:</p> <pre>arcsight resvalidate</pre> <pre>arcsight resvalidate -persist false</pre>
----------	---

ruledesc

Description	This command is a rule description tool to fetch rules information. (Used by HPOVO.) Tool to monitor managed objects in the Manager.	
Applies to	Manager	
Syntax	ruledesc -t {ovo uri} -i info [parameters]	
Parameters	-t <type>	(Required) The type can be ovo, or uri.
	-i <info>	(Required) Info (depends on type).
	-m <host>	Manager host name or address
	-p <pwd>	Password
	-port <port>	Port for Manager. Default: 8443
	-prot <prot>	The protocol can be http, or https. If none is specified, the default is https.
	-u <name>	User name
Examples	<p>To run:</p> <pre>arcsight ruledesc</pre>	

runcertutil

Description	<p>This command is a wrapper launcher for the NSS <code>certutil</code> tool used for managing certificates and key pairs. For more details on the <code>certutil</code> 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

runcertutil, continued

	-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 -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, 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

runcertutil, continued

	-k <key_type>	Type of key pair to generate. The normal option is -k rsa. If you are using FIPS Suite B, use -k ec -q secp<bits>r1. The value of <bits> is 256 for up to secret classifications and 384 for up to top secret classifications. You can use 521, but some browsers cannot handle the 521-bit algorithm. See "Types of Key Pairs Used in FIPS Mode" on page 156 .
	-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	This command is 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	
	-fips [true false]	Alias for the certificate
Parameters	-dbdir <dir_path>	The security database directory
	-H	Help on this tool
Examples	To run: arcsight runmodutil	

runpk12util

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

script

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

searchindex

Description	<p>This command creates or updates the search index for resources.</p> <p>If you provide the credentials for the Manager, it automatically associates with the newly created or updated index. However, if you do not specify any credentials, manually configure the Manager to use the updated index.</p>	
Applies to	Manager	
Syntax	<code>searchindex -a action</code>	

searchindex, continued

Parameters	-a <action>	<p>Possible actions: create, update, or regularupdate</p> <p>create—Creates a new search index.</p> <p>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.</p> <p>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.</p>
	-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	<p>To run:</p> <pre>arcsight searchindex -a <action></pre>	

Note: 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	This command runs a 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

sendlogs, continued

Syntax	sendlogs	
Parameters	-f <file>	Log file name (properties file in -i silent mode)
	-g	Generate sample properties file for -i silent mode
	-i <mode>	The mode can be console, silent, recorderui, or swing.
	-n <num>	Incident number (Quick mode)
Examples	arcsight sendlogs	

tee

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

tempca

Description	This command allows you to 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

tempca, continued

	-i	Display summary of current SSL settings
	-k <n>	Key store: Manager (1)
	-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	This command extracts and reformats thread dumps from the file to which you wrote the thread dumps in the <code>managertthreaddump</code> command (<code>manager/logs/default/server.std.log</code>). 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	This command is a standalone Velocity template processor.	
Applies to	Manager	
Syntax	tproc	
Parameters	-d <file>	Definitions file

tproc, continued

	-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	

whois

Description	This command is used by the whois command of the console	
Applies to	Console	
Syntax	whois [-p <port>] [-s <host>] <target>	
Parameters	-p <port>	Server port
	-s <host>	Name or address of 'whois' server
	<target>	Name or address to lookup
Examples	To run: arcsight whois	

zoneUpdate

Description

This command updates IPv4 address allocations and dark space information that are provided in the periodic Zone Update Subscription Package, contained in the . Zone_Updates_<version>.zip file. Then, at the command line, run the zoneUpdate command to apply the zone updates. Use of this command is optional.

You can use zoneUpdate after a successful Manager installation or upgrade. This command is available from the command line only, and has no GUI functionality.

zoneUpdate performs these actions in the Global network:

- Makes an inventory of affected assets
- Removes old zones
- Installs and updates zones
- Auto-zones assets that appeared in the inventory of affected assets in the Global network

zoneUpdate updates zones in the Global network only. Local zones are not updated by this command. The behavior of zoneUpdate is the same for both dynamic and static zones.

Recommendations

- HP recommends that assets are allocated to the local network only and that the Global network does not contain assets. Also, zones that have categories assigned to them, and then are removed and reinstalled as part of the zone update process lose the category assignments. HP also recommends you do not assign categories to the system zones.
- HP recommends that you perform a full system database table backup (export_system_tables) and export the current ArcSight Network package before using zoneUpdate, to ensure that you have a usable snapshot of your network model. If the zone update process is interrupted or a problem occurs and you must revert your data, be sure to use this backup to restore your ArcSight resources before attempting to run zoneUpdate again.
- HP recommends running zoneUpdate during non-peak system time.

Running zoneUpdate

Note: Zone Groups belonging to Regional Internet Registries (RIR) that contain more than 1000 zones will place their corresponding zones in subgroups, each group containing up to 950 zones, to enable you to better manage those zones, and content related to them, from within the ArcSight Console.

1. Log in as user *arcsight*.

zoneUpdate, continued

2. Verify that the Manager is running.
3. Extract the Zone_Updates_<version>.zip file into a directory. The directory can be of your choice. The zipped files extract into the folder ArcSight_Networks_<version>, which contains the files ArcSight_Networks.arb and Zone_Removal_Tool.xml. Do not change the name of this folder or the names of the extracted files.
4. Verify that the user *arcsight* has write permissions to the directory into which you extracted Zone_Updates_<version>.zip.
5. As user *arcsight*, run this command:

```
/opt/arcsight/manager/bin/arcsight zoneUpdate -m <Manager hostname or IP address> -u admin -f <folder where zip file was extracted>
```

You are prompted for the user password. **Be sure to enter the correct password.** zoneUpdate uses the entered password several times, and temporarily locks you out if you use the wrong password. If this happens, you can reenableView the user or wait for the user to be reenableView automatically.

Running zoneUpdate can take up to 20 or 40 minutes, depending on Manager workload and the number of assets assigned to the Global network.

Note: If a user with administrative privileges is not logged into the ArcSight Console or ACC before the zoneUpdate process is launched, that user will not be able to log in until zoneUpgrade is complete. Other users, including the members of Administrators group, will be able to log in at any time while zoneUpdate is running.

Warning: Do not interrupt or kill zoneUpdate after the process starts. Allow zoneUpdate to complete, and then make a determination of the condition of your zones and whether to install another version of the Zone Update Subscription package.

Recovery and Troubleshooting

Zone Updates Not Applied

If zoneUpdate runs with errors, and does not apply the zone updates from the Zone Update Subscription Package, follow these steps:

1. Restart the Manager.
2. Run zoneUpdate again.
3. If the above steps do not work, and you encounter the same errors as before, import the full system database table backup (export_system_tables) and the current ArcSight Network package that you exported before initially running

zoneUpdate, continued

	<p>zoneUpdate.</p> <p>4. Run zoneUpdate again.</p> <p><i>Package Exists Error When Applying the Zone Update Subscription Package</i></p> <p>If you encounter these messages when running zoneUpdate:</p> <pre>Reading bundle 'Common Bundle Alias' Done. 0 min 0 sec 41 ms Importing 1 packages Importing package 1/1 '/All Packages/ArcSight System/ArcSight Networks' Parsing archive 'ArcSight Networks.xml'... Done. 0 min 1 sec 19 ms Package Already Exists with Newer Content</pre> <hr/> <pre>Package '/All Packages/ArcSight System/ArcSight Networks' already exists in the system with newer content 1: Leave newer package 2: Never override newer packages 3: Update package 4: Always update Packages 5: Abort</pre> <hr/> <p>Choose option 3, Update Package.</p> <p>Asset Zoning</p> <p>Assets that were zoned in the Global network before you run zoneUpdate will be zoned after the command completes.</p> <p>Asset Ranges</p> <p>Asset ranges are not auto-zoned by zoneUpdate. Asset ranges will be unzoned by the running of the zoneUpdate; you must manually rezone asset ranges after you run zoneUpdate if you had asset ranges in the Global network.</p> <p>For example, if you had an asset range in Zone A in a previous version of ESM, the asset range is unzoned after you run zoneUpdate. For this example, suppose Zone A was split into two zones, Zone A and Zone B, and after upgrade your asset range spans the last part of Zone A and first part of Zone B. In this case, the asset range becomes unzoned. To recover zoning, you must open each unzoned asset range resource and map it to the correct zone, or split it into two asset ranges that map to the new Zones A and B.</p>
Applies to	Manager, Console
Syntax	/opt/arcsight/manager/bin/arcsight zoneUpdate -m <Manager hostname or IP address> -u admin -f <folder where zip file was extracted>

zoneUpdate, continued

Parameters	-m <manager>	The Manager hostname or IP address. Use of a hostname or an IP address depends on whether your Manager was configured using a hostname or an IP address.
	-u <username>	The name of a user with administrative privileges.
	-f <folder>	Folder name or the path to the folder that contains the unzipped Zone Update Subscription package. For example, /opt/arcsight/manager. Extract the file Zone_Updates_<version>.zip into this folder, and give the folder write permission.
	-h	Help
Example	<p>To update zones:</p> <pre>/opt/arcsight/manager/bin/arcsight zoneUpdate -m 192.0.2.0 -u admin -f /opt/arcsight/manager</pre>	

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 configbackup 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 configs.tar.gz which you can find in opt/arcsight/logger/current/arcsight/logger/tmp/configs.	
Applies to	CORR-Engine	
Syntax	arcsight configbackup	
Parameters	none	

configbackup, continued

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 <code>configbackup</code> command.	
Applies to	CORR-Engine	
Syntax	<code>arcsight disasterrecovery start</code>	
Parameters	<code>start</code>	
Example	To run: <code>/etc/init.d/arcsight_services stop logger_servers</code> <code>cp ~/configs.tar.gz</code> <code>/opt/arcsight/logger/current/backups/configs.tar.gz</code> <code>/opt/arcsight/logger/current/arcsight/logger/bin/arcsight</code> <code>disasterrecovery start</code> <code>/etc/init.d/arcsight_services start logger_servers</code>	

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 a machine where the following characteristics are exactly the same as the backup machine:

- The version of ESM must be the same
- The version of the operating system (and the time zone to which it is set) must be the same
- The archive locations for the backed-up storage groups must already exist and be the same
- The MySQL password must be the same

exportdatausage

Description	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. Note: This command has to be run from a different location than the other <code>arcsight</code> commands. Run it from: <code>/opt/arcsight/logger/current/arcsight/logger/bin</code>	
Applies to	CORR-Engine	
Syntax	<code>exportdatausage <path/file></code>	
Optional Parameter	<code><path/file></code>	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 <code>.csv</code> extension. If you do not specify this parameter, the data is displayed on screen.
Examples	To create a file called <code>usagefile.csv</code> in <code>/opt/arcsight</code> , run: <code>arcsight exportdatausage /opt/arcsight/usagefile</code>	

Appendix B: Troubleshooting

The following information may help solve problems that occur while operating the ArcSight system. In some cases, the solution can be found here or in specific ArcSight documentation, but Customer Support is available if you need it.

If you intend to have Customer Support guide you through a diagnostic process, prepare to provide specific symptoms and configuration information.

General

You changed your File system format from XFS to EXT4 or back and now you have problems.

Note: You cannot change the file system for the ESM Express appliance.

Both XFS and EXT4 file system formats are supported during installation. However, ESM configures itself to the file system upon which it is first installed; you therefore cannot change file system type after installation, even during an upgrade. Roll your file system back to what it was before.

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 ["Running the Manager Configuration Wizard" on page 80](#).

Report is empty or missing information

Check that the user running the report has inspect (read) permission for the data being reported.

Running a large report crashes the Manager

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the Manager to crash and restart. To prevent this scenario, you can set up the Manager to expose a special report parameter for generating the report in a separate process. The separate process has its own VM and heap, so the report is more likely to generate successfully. Even if the memory allocated is still not enough, the report failure 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.canarchiveinseparateprocess=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 VM.

Note: Use this parameter only if you experience a Manager crash when running large reports such as the ones that contain tables with more than 500,000 rows and 4 or 5 columns per row.

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>/i18n/server/reportpdf_config_<locale>.properties` file. You have the option to change the default mapping of any TrueType font to the OpenType font by modifying the respective font mapping in this file.

To work around the issue of mangled fonts, ArcSight recommends that you:

1. Install a localized Adobe Reader 8.0 depending on the language of your platform on your Manager machine. This version of the Adobe Reader installs the OpenType fonts by default.
2. Edit the `server.properties` file as follows:
 - a. Set `report.font.truetype.path` property to point to the directory that contains the TrueType and OpenType font. 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.

Event IDs have negative numbers

Negative event ID numbers can occur, and are normal. Event IDs are 64-bit values. The less-significant 48 bits are assigned to a newly received event by the receiving Manager; these bits uniquely identify the event in the database of that Manager. The more-significant 16 bits are used to store forwarding information. When an event ID with '1' in the topmost bit is represented as Java 'long' value, the event ID value is interpreted as a negative number according to JVM rules. When displayed, such an event ID appears as a decimal number with a sign '-' in front of it.

Pattern Discovery Performance

Note: Pattern Discovery is not supported on the ESM Express appliance.

Time spread calculations can take up a lot of CPU time, especially if Pattern Discovery has been running for a long time. If performance is degraded as a result of this feature, you can find out by checking the `system.log` for the start and end times of the Pattern Discovery process. If it is taking longer than expected, and if that is a problem for you, turn the Time Spread feature off.

To turn it off, add the property `patterns.timeSpreadCalculation=False` to the Manager's `server.properties` file.

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. After 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 trend 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 trend:

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

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.

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.

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.

Services do not start after a power failure during "start all"

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

To resolve the problem, delete the postgresql lock file. The location of the postgresql lock file, is given in the pgsqll log file in `/opt/arc sight/logger/userdata/logs/pgsqli/serverlog`. If this problem occurs, the text "could not create lock file" can be written to the server log. To verify, search the server log for instances of the text "could not create lock file".

Reboot the server after removing the postgresql lock file.

Asset aging not working as expected (not all aged assets deleted)

If you are using ESM's asset auto-deletion feature to remove assets from the system, some aged assets may remain in the system. This can occur in environments that have more than 10,000 assets in an asset group. HP ArcSight recommends not to exceed 10,000 resources for any resource group. If there are more than 10,000 assets in a group, the auto-deletion process slows down and times out without deleting these assets. For details on asset aging see, ["Asset Aging" on page 40](#).

To solve this problem, you can set certain `asset.aging.task` parameters to gradually delete the unwanted aged assets off of the system. This gradual deletion allows you to delete a relatively small number of assets at a time, keeping the transaction time short and the database load low while the cleanup occurs. This process will gradually delete the aged assets, but can take several days, depending on the number of assets involved and the system load. Stop the manager before making the parameters changes and restart it when you are done; see the chapter ["Configuration" on page 15](#) for details on stopping and starting the Manager.

To configure the Manager to start the gradual asset deletion process:

1. Add the following properties to the `server.properties` file (in this example, assets will be aged after 4 days and 500 assets will be deleted each hour). See [" Editing Properties Files" on page 16](#) for details.


```
asset.aging.daysbeforedisable=4
asset.aging.task.operation=delete
asset.aging.task.maxassetsprocess=500
asset.aging.task.maxassetsload=500
asset.aging.task.period=Hourly
asset.aging.task.minute=0
```

Notes:

- For the property `asset.aging.daysbeforedisable` note that the default value of -1 means that asset aging is turned off, not that assets will be disabled and deleted. The value for `asset.aging.daysbeforedisable` is expressed in days that define how long an asset is allowed to age before it is disabled and deleted.
 - For the deletion of aged assets to work properly, verify that the `asset.aging.task.operation` property is set to `delete`.
 - Set the properties `asset.aging.task.maxassetsprocess` and `asset.aging.task.maxassetsload` to the same value. The value depends on your hardware and system load. The higher the number specified, the faster the asset deletion will occur. We recommend starting with the value 500 for these two properties, and after the number of assets falls to around 100,000, you can try increasing these properties to 1000.
2. In the `server.defaults.properties` file, verify the value of the property `dbconmanager.provider.logger.pool.maxcheckout`. If the value is less than 3600, add this line to the `server.properties` file:
`dbconmanager.provider.logger.pool.maxcheckout=3600`
 3. Monitor the progress of the asset deletion. When the desired asset limit is reached, stop the process by deleting the properties you added to the `server.properties` file (`asset.aging.daysbeforedisable`, `asset.aging.task.operation`, `asset.aging.task.maxassetsprocess`, `asset.aging.task.maxassetsload`, `asset.aging.task.period`, `asset.aging.task.minute`, and `dbconmanager.provider.logger.pool.maxcheckout`).

The property settings described above are not standard configurations. In the future, monitor the number of assets in groups and do not let them exceed the recommended maximum of 10,000 resources for any resource group.

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 are not 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.

CORR Engine - Temporary Sort Space 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. 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 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 "[View Certificate Details From the Store](#)" on page 57.

Appendix C: Creating Custom E-mails Using Velocity Templates

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

A sample use case is presented to illustrate the concept.

Velocity Templates

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. 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.  
  
#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

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  
-----
```

After 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>

Appendix D: Configuration Changes Related to FIPS

This appendix provides information about and instructions for configuring ESM to support Federal Information Processing Standard (FIPS) 140-2, Suite B, and some other configuration changes you can make while in FIPS mode.

FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. A cryptographic module is either hardware or software or a combination that is used to implement cryptographic logic. The US federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet the FIPS standard.

- To be compliant with FIPS 140-2, all components, including Connectors and Logger, if present, must be configured in FIPS mode. Connectors and Logger setup are covered in their documentation.
- For information about supported platforms and specifics about FIPS mode architecture for all ESM products, contact ArcSight Customer Support.
- TLS is based on SSL 3.0, for a better understanding of how SSL works. Read ["SSL Authentication" on page 44](#).

Tools Used to Configure Components in FIPS

Network Security Services (NSS) is a cross-platform cryptographic C library and a collection of security tools. ESM comes bundled with the following three basic NSS command line tools:

- `runcertutil` - is a certificate and key management tool used to view and generate key pairs and certificate signing requests (CSR) and import and export public certificates from key pairs.
- `runmodutil` - is the NSS module configuration tool. It is used to enable or disable the FIPS module and change key store passwords.
- `runpk12util` - is an import and export tool for PKCS #12 format key pairs (.pfx files).

See ["Administrative Commands" on page 88](#) for details on the above command line tools. You can also refer to the 'NSS Security Tools' page on the Mozilla website for more details on any of the above NSS tools (search for them as `certutil`, `modutil`, or `pk12util`).

For online help on any command, enter the following command from a component's `\bin` directory:

```
./arcsight <command_name> -H
```

FIPS Encryption

A cipher suite is 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 in FIPS:

- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

The following cipher suites are enabled for FIPS Suite B:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Types of Key Pairs Used in FIPS Mode

The type of key pair for FIPS 140-2 mode is the same type used in non-FIPS mode. When using the `runcertutil` command, the key-type option would be `-k rsa`.

The type of key pair for FIPS with Suite B is different. The key type depends on the level of classification you need to accommodate. FIPS Suite B requires the use of elliptic curve cryptography so the key-type option starts out `-k ec`. After that you have to specify the `-q secp<bits>r1` option. The value of `<bits>` is:

- 256 -- for up to secret classifications corresponding to 128-bit encryption
- 384 -- for up to top secret classifications corresponding to 192-bit encryption

For example, if you are generating a key pair on the Manager, you might use a command like this:

```
./arcsight runcertutil -S -s "CN=<previous_CN>" -v <validity_in_months> -n mykey -k ec -q secp384r1 -x -t "C,C,C" -m 1234 -d /opt/arcsight/manager/config/jetty/nssdb
```

You can use `secp521r1`, but some browsers, such as Internet Explorer 11 (on Windows 8.1 and Windows Server 2012) and Chrome (on any operating system), cannot use the 521-bit option. The examples in this document use 521, but if you are using IE 11 on those OS versions or Chrome, then use `secp384r1`.

Types of Certificates Used in FIPS Mode

When dealing with certificate based identification and encryption, components fall into one of two categories: servers and clients. Signed certificates enable these components to verify the validity of

communications with the other components. You can use either a self-signed certificate or a CA-signed certificate when setting up SSL authentication on your ESM components.

Using a Self-Signed Certificate

When you use a self-signed certificate, the public part of the server's key is used to identify and encrypt communications between the client and server. A self-signed certificate is automatically generated when doing a fresh installation of ESM.

Using a Certificate Authority (CA) Signed Certificate

In a configuration using a CA-signed certificate, the public part of the server's key is sent to the client and the client identifies it using the Certificate Authority's root certificate. The root certificate identifies the validity of the certificate by matching itself against the Issuer section of the public certificate.

To obtain a CA signed certificate there are two options.

1. Buy or obtain a keypair from a Certificate Authority (CA). When putting in server data for your new server certificate, verify that the Subject Common Name (CN) matches the Fully qualified hostname (FQDN) or IP address of your server.
2. From your Manager, Generate a Certificate Signing Request (CSR). Send the CSR to a Certificate Authority and retrieve the new keypair from the CA.

After acquiring your new CA Signed Keypair, import it into the nssdb using the `runpkcs12util` utility.

For all clients connecting to the server that uses the CA signed certificates, import the CA's root certificate. It will be used to validate the certificate from the server.

The instructions in this section for converting from the default self-signed certificates to a CA signed certificate assume that the Manager is already running in FIPS mode.

Steps Performed on the Manager

Below are the steps to configure your ArcSight server application to use a CA signed certificate in FIPS 140-2 mode.

1. Stop the Manager.
2. Find out what the common name is.
3. Delete any previously imported/generated Manager certificate or key pair. (Make sure you know the common name (CN) it uses before you delete it, because the new certificate needs to use the same CN.)

```
./arcsight runcertutil -D -n mykey -d  
/opt/arcsight/manager/config/jetty/nssdb
```

4. Generate a certificate signing request (CSR) by running the following from the Manager's /bin directory:

To create a PEM ASCII format CSR file:

```
./arcsight runcertutil -R -s "CN=<previous_CN>, O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>, ST=<State_where_organization_is_  
located>, C=<Country>" -a -o <absolute_path_to_filename.csr> -d  
/opt/arcsight/manager/config/jetty/nssdb
```

For Suite B, add -k ec -q secp521r1 as follows:

```
./arcsight runcertutil -R -s "CN=<previous_CN>, O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>, ST=<State_where_organization_is_  
located>, C=<Country>" -k ec -q secp521r1 -a -o <absolute_path_to_filename.csr>  
-d /opt/arcsight/manager/config/jetty/nssdb
```

For more information on the -q secp521r1 option, see ["Types of Key Pairs Used in FIPS Mode" on page 156](#).

Note: If you do not specify the absolute path to where the .csr file should go, the path specified for the output file will be relative to <ARCSIGHT_HOME> (/opt/arcsight/manager).

To create a DER binary file:

```
./arcsight runcertutil -R -s "CN=<hostname_or_IP>, O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>, ST=<State_where_organization_is_  
located>, C=<Country>" -o <absolute_path_to_filename.csr>  
-d /opt/arcsight/manager/config/jetty/nssdb
```

Enter the password for the NSS DB when prompted. The default is described in ["NSS database password" on page 47](#).

Enter random keyboard strokes when prompted to generate the random seed to generate your key.

The CSR is generated in the location specified by the -o option.

5. Send the .csr file to your Certificate Authority.

The Certificate Authority validates the content of the submitted certificate request (CSR) and signs the certificate with the CA root certificate.

6. After you receive the signed certificate from the CA, import it into the Manager's NSS DB by running these commands from the Manager's /bin directory:

```
./arcsight runcertutil -A -n mykey  
-t "C,C,C" -d /opt/arcsight/manager/config/jetty/nssdb -i <absolute_path_to_  
the_signed_certificate>
```

7. Start the Manager by running the following command as user *arcsight*:

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

Steps Performed on the ArcSight Console

You are required to import the CA root certificate into the Console's `nssdb.client`. This allows the Console to trust the Manager.

Note: Make sure that you have copied the CA root certificate to the machine on which you install the ArcSight Console.

1. Import the root certificate from the Certificate Authority (CA) used to sign the managers certificate by running:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert>  
-t "CT,C,C" -d <ARCSIGHT_HOME>\current\config\nssdb.client -i <path_to_the_  
CA's_root_certificate>
```

For the `-t` option, be sure to use CT,C,C permission flags only and in the order shown above.

2. Start the Console. You should see a message saying that the Console is starting in FIPS mode.

Some Often-Used SSL-Related Procedures

Here are some of the commonly used SSL-related procedures that are intended to serve as a reference when installing or setting up ESM components in FIPS mode.

Generating a Key Pair in a Component's NSS DB

Note: When you import or generate a key pair in a component's NSS DB, if there is an existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility uses the existing alias for the newly created key pair and ignores the alias you supplied in the `runcertutil` command line.

This section explains how to generate a key pair in a component's NSS DB. A component that has to authenticate itself is required to have a key pair on it. For example, during server-side authentication, since the server needs to authenticate itself to a client, the server should have a key pair in its NSS DB and send its certificate which contains the server's public key to the client requesting it. The same is true for client-side authentication where a key pair has to exist on the client. For self-signed certificate, the certificate gets generated when generating a key pair.

On the Manager

1. Run the following command from the Manager's <ARCSIGHT_HOME>/bin directory to generate a key pair. Make sure there is no other key in the Manager's NSSDB:

```
./arcsight runcertutil -S -s "CN=<hostname>" -v <number_of_months_the_certificate_should_be_valid> -n mykey -k rsa -x -t "C,C,C" -m 1234 -d /opt/arcsight/manager/config/jetty/nssdb
```

Note: Hints on generating a key pair:

- Make sure to use *mykey* as the alias name for the key pair as shown in the example.
- The *-m* serial number should be unique within *nssdb*.
- The hostname is the short name or fully qualified domain name depending upon how your Manager name was set up when you installed the Manager.
- Using *-v* to set the validity period of your certificate is optional. If you choose to use it, see ["Setting the Expiration Date of a Certificate" on page 167](#) for details. To see the validity period of an existing certificate, see ["View Certificate Details From the Store" on page 57](#).

In the above command, the hostname is the name of the machine on which your Manager is installed and *-v* is the validity period of the certificate.

For example, if your hostname is *myhost.arcsight.com*, you would run:

```
./arcsight runcertutil -S -s "CN=myhost.arcsight.com" -v 6 -n mykey -k rsa -x -t "C,C,C" -m 1234 -d /opt/arcsight/manager/config/jetty/nssdb
```

This generates a key pair and certificate with the alias *mykey* which is valid for 6 months from the current date and time in the Manager's *nssdb*.

2. Enter the password for NSS DB when prompted. The default is described in ["NSS database password" on page 47](#).
3. Enter random keyboard strokes when prompted, to generate the random seed used to generate your key.

On the Console

To create a key pair on the Console:

1. Run the following command from console's /bin directory:


```
./arcsight runcertutil -S -s "CN=<hostname>" -v <number_of_months_the_
certificate_should_be_valid> -n <provide_an_alias_name_for_the_key> -k rsa -x -
t "C,C,C" -m 2345 -d <ARCSIGHT_HOME>\config\nssdb.client
```

If you are using Suite B, use `-k ec -q secp521r1` instead of `-k rsa`.

Where:

- `<hostname>` is the name of the machine on which console is installed.
 - Using `-v` is optional. If you use it, see ["Setting the Expiration Date of a Certificate" on page 167](#) for details.
 - The `-m` serial number must be unique within `nssdb.client`. In this case, 2345 is just an example.
 - See ["Types of Key Pairs Used in FIPS Mode" on page 156](#) for more information on the `secp521r1` option.
2. Enter the password for `nssdb.client`. The default is *changeit*.
 3. Enter random keyboard strokes when prompted, to generate the random seed used to generate your key.

Verifying Whether the Key Pair Has Been Successfully Created

To verify whether the key pair has been successfully created in the `nssdb`, run the following from the component's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -d <path_to_the_component's_NSS_DB>
```

Note: When you import or generate a key pair into NSS DB, if there is an existing key pair/certificate with the same CN as the one you create, the `runcertutil` utility uses the existing alias for the newly created key pair and ignores the alias you supplied in the `runcertutil` command line.

Viewing the Contents of the Manager Certificate

If you would like to check the contents of the certificate, you run this from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <path_to_the_component's_NSS_DB> -n mykey
```

Exporting Certificates

This section explains how to export a certificate from a component's NSS DB. During an SSL handshake, for server side authentication, have the server's certificate in the NSS DB of both the server and the client. Export the server's certificate from the server's NSS DB to import it into the client that wishes to connect to the server.

Likewise, for client side authentication, have the client's certificate in the NSS DB of both the client and the server. Export the client's certificate from the client's NSS DB to import it into the server to which the client connects.

Exporting a Certificate From the Manager

Run the following command from the Manager's <ARCSIGHT_HOME>/bin directory:

```
./arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d  
/opt/arcsight/manager/config/jetty/nssdb -o <absolute_path_to_where_you_want_  
certificate_exported>
```

For example:

```
./arcsight runcertutil -L -n mykey -r -d /opt/arcsight/manager/config/jetty/nssdb -  
o /home/arcsight/arcsight/Manager/ManagerCert.cer
```

This exports the Manager's certificate into a file called ManagerCert.cer and places it in your /home/arcsight/arcsight/Manager directory. The alias for this file is mykey.

Note: If you do not specify the absolute path for the .cer file, it is placed in the Manager's <ARCSIGHT_HOME> directory.

Exporting a Certificate From the Console

To export the Console's certificate run the following from the Console's \bin directory:

```
arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d <ARCSIGHT_  
HOME>\current\config\nssdb.client -o <absolute_path_to_where_you_want_certificate_  
exported>
```

Note: If you do not specify the absolute path for the .cer file, it is placed in the Console's <ARCSIGHT_HOME> folder.

Importing a Certificate into the NSS DB

This section explains how to import a certificate into a component's NSS DB. For server side authentication, import the server's certificate into the client's NSS DB. For client side authentication, the client's certificate needs to be imported into the server's NSS DB.

Use `runcertutil` to import a certificate into the NSS DB.

On the Manager

If you use a CA-signed certificate, import the Manager's CA-signed certificate into the Manager's `nssdb`. In addition, if you set up client side authentication, import the client's certificate into the Manager's `nssdb`. Import a certificate into the Manager's `nssdb` by running:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_certificate> -t "CT,C,C" -d  
/opt/arcsight/manager/config/jetty/nssdb -i <absolute_path_to_the_certificate_file>
```

For the `-t` option, be sure to use CT,C,C permissions flags only and in the same order that it is shown above.

If you are importing the Console's certificate to set up client-side authentication, make sure that you do NOT use the alias `mykey` for the Console's certificate when importing it into the Manager's `nssdb` because the `nssdb` already has the Manager's certificate with the alias `mykey` in it. All aliases in the `nssdb` should be unique.

On the Console

Import the Manager's certificate into the Console that connects to the Manager. To import a certificate into the Console's `nssdb.client`:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t "CT,C,C" -d  
<ARCSIGHT_HOME>\config\nssdb.client -i <absolute_path_to_certificate_file>
```

For the `-t` option, be sure to use CT,C,C permissions flags only and in the same order that it is shown above.

Importing an Existing Key Pair into the NSS DB

If you already have an existing key pair, you can use it instead of generating a new key pair on a component. This procedure instructs you how to import an existing key pair into a component's NSS DB.

1. Export the key pair using a tool, such as `keytoolgui`, and be sure to export the key pair with the name you gave it. An alias is required in order to import the key pair into NSS DB.
2. Import the `.pfx` file into NSS DB using the `runpk12util` tool. Make sure that the alias of the key pair being imported does not match the alias of a pre-existing key pair in the component's NSS DB. If the alias of the key pair being imported matches the alias of a pre-existing key pair in the component's NSS DB, the new keypair is imported with a different alias generated by the tool. The new alias is displayed on the screen.

Run the following command from the component's `/bin` directory

On the Manager:

```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d  
/opt/arcsight/manager/config/jetty/nssdb
```

On the Console:

```
arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d <ARCSIGHT_  
HOME>\current\config\nssdb.client
```

3. Run the following from the component's <ARCSIGHT_HOME>/bin directory to verify that the key pair has been imported correctly. Note that the alias of the key pair that you just imported in the NSS DB is the same as the alias of that key pair in the .pfx file, in our example, mykey.

On the Manager:

```
./arcsight runcertutil -L -d /opt/arcsight/manager/config/jetty/nssdb
```

You should see the alias of the imported key pair in the output.

Setting up Server-Side Authentication

When you install a component in FIPS mode, you set it up for server-side authentication. Setting up client-side authentication is optional.

Setting up Client-Side Authentication

SSL 3.0 supports client-side authentication. TLS is based on SSL 3.0. ESM uses TLS and supports client-side authentication.

The client side authentication takes place after the initial handshake (after the Manager has authenticated itself to the Console). The Manager then requests the Console for its (Console's) certificate. The Console in turn sends its certificate to the Manager. The Manager has to be configured to accept the Console's certificate. In other words, the Console's certificate must exist in the Manager's nssdb prior to the Manager authenticating the Console. With this high level overview in mind, here are the steps you need to perform to set up client-side authentication.

If you plan to use self-signed certificate for the Console:

1. Stop the Console if it is running.
2. Use an existing key pair which you import into the Console's NSS DB from another component. See ["Importing an Existing Key Pair into the NSS DB" on the previous page](#) for details.
3. Export the Console's certificate. See the section ["Exporting Certificates" on page 162](#) ("From the Console" subsection) for detailed instructions.
4. Stop the Manager if it is running.

5. Import the Console's certificate into the Manager's nssdb. See the section ["Importing a Certificate into the NSS DB" on page 162](#) ("On the Manager" subsection) for details.

Caution: Make sure that you do NOT use the alias mykey for the certificate when importing it into the Manager's nssdb because the nssdb already has the Manager's certificate with the alias mykey in it. All aliases in the nssdb must be unique.

6. Restart the Manager, then Console.

If you plan to use CA-signed certificate for the Console:

1. Stop the Console if it is running.
2. Generate a CSR on the Console by running the following from the Console's \bin directory:

```
arcsight runcertutil -R -s "CN=<hostname_or_IP>, O=<Name_of_organization>,  
L=<City_where_the_organization_is_located>, ST=<State_where_organization_is_  
located>, C=<Country>" -a -o <absolute_path_to_filename.csr>  
-d <ARCSIGHT_HOME>\current\config\nssdb.client
```

Note: If you do not specify the absolute path to where you want the .csr file to be placed, the .csr file is placed in the Console's <ARCSIGHT_HOME>.

3. Send the CSR file to your CA and obtain a signed certificate from your CA.
4. Import the CA-signed certificate into the Console's nssdb.client. Run:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t "C,C,C" -d  
<ARCSIGHT_HOME>\config\nssdb.client -i <absolute_path_to_certificate_file>
```

5. Stop the Manager if it is running.
6. Import the root certificate from the Certificate Authority (CA) used to sign the console certificate into the manager's nssdb by running:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t "CT,C,C" -d  
/opt/arcsight/manager/config/jetty/nssdb -i <path_to_the_CA's_root_certificate>
```

7. Restart the Manager.

Changing the Password for NSS DB

ESM ships with a default password for the NSS DB (see ["NSS database password" on page 47](#)). HP recommends that you change the password on each component before moving to a production environment. (You can have different passwords for each component.) To do so:

1. Disable the FIPS mode in NSS DB by running the following from the component's /bin directory:

```
./arcsight runmodutil -fips false -dbdir <absolute_path_to_the_component's_NSS_DB>
```

2. Run the following to list the NSS DB's token name:

```
./arcsight runmodutil -list -dbdir <absolute_path_to_the_component's_NSS_DB>
```

3. Change the token's password by running the following from the component's /bin directory:

```
./arcsight runmodutil -changepw "<name_of_token>" -dbdir <absolute_path_to_the_component's_NSS_DB>
```

4. Enter the old password and a new password and confirm it when prompted.

5. Re-enable FIPS mode on the NSS DB:

```
./arcsight runmodutil -fips true -dbdir <absolute_path_to_the_component's_NSS_DB>
```

6. If you changed the password on the Manager, run the following commands:

from /opt/arcsight/manager/bin:

```
./arcsight changepassword -f /opt/arcsight/manager/config/server.properties -p  
servletcontainer.jetty311.truststore.password
```

Then run

```
./arcsight changepassword -f /opt/arcsight/manager/config/server.properties -p  
server.privatekey.password
```

Restart the Manager

7. If you changed the password on the ArcSight Console, run the following commands from the ArcSight Console's <ARCSIGHT_HOME>\current\bin folder:

```
arcsight changepassword -f <ARCSIGHT_HOME>\current\config\client.properties -p  
ssl.keystore.password
```

Then run:

```
arcsight changepassword -f <ARCSIGHT_HOME>\current\config\client.properties -p  
ssl.truststore.password
```

Listing the Contents of the NSS DB

After you import a certificate or generate a key pair in a component's NSS DB, you can verify that the certificate import was successful or the key pair has been successfully generated. You can do this by

listing the contents of the NSS DB. To view the contents of a component's NSS DB, run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <absolute-path-to-the_component's_NSS_DB>
```

You should see the alias of the certificate you just imported or the alias for the key pair you generated.

Viewing the Contents of a Certificate

To view the contents of a certificate, run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -L -d <absolute-path-to-the_component's_NSS_DB> -n  
<certificate_alias>
```

Setting the Expiration Date of a Certificate

To set the expiry date of the certificate, do it when generating the key pair. After you have generated the key pair, you cannot change the expiration date on the certificate and the certificate expires in three months by default.

```
./arcsight runcertutil -S -s "CN=<hostname>" -v <number_of_months_the_certificate_  
should_be_valid> -n mykey -k rsa -x -t "C,C,C" -m 1234 -d <component's_NSS_DB_path>
```

You specify the validity of the certificate with the `-v <number_of_months>` option. The value that you provide with `-v` calculates the number of months that the certificate is valid starting from the current time. You can use the `-w <offset_months>` along with `-v` to set the beginning time for the validity. The `-w <offset_months>` if used, calculates the start time of the certificate validity and the offset is calculated from the current system time. If you do not use the `-w` option, the current time is used as the start time for the certificate validity. See the subsection, "runcertutil" in ["Administrative Commands" on page 88](#) for details on the `-v` and `-w` options.

Deleting a Certificate from NSS DB

To delete a certificate from a component's NSS DB:

1. Stop the component if it is running.
2. Run the following command from the component's `/bin` directory:

```
./arcsight runcertutil -D -n <certificate-alias> -d <absolute-path-to-the_  
component's_NSS_DB>
```

Replacing an Expired Certificate

When an existing certificate/nssdb expires on the Manager server, replace it with a new one. You can see when a certificate expires by opening it.

To replace the certificate:

1. Stop all services by running the following command (as user *arcsight*):

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

2. Delete the expired certificate from the server's NSS DB. See ["Deleting a Certificate from NSS DB" on the previous page](#) for details.

Since the common name (CN) for the new certificate is identical to the CN in the old certificate, the expired and new certificates cannot co-exist in the NSS DB.

3. In case of CA-signed certificate, replace the certificate by importing the new certificate into the server's NSS DB.

In case of self-signed certificate, generate a key pair on the server. See ["Generating a Key Pair in a Component's NSS DB" on page 159](#) for details on how to do this. Generating the key pair automatically generates the certificate.

4. On every client that connects to the server, make sure to delete the old expired server certificate from the client's NSS DB and import the server's newly generated certificate.

For example, if your Manager's certificate has expired, do the following:

- a. Delete the expired certificate from the Manager's nssdb. See ["Deleting a Certificate from NSS DB" on the previous page](#)
- b. Generate a new key pair, which automatically generates a new self-signed certificate. See ["Generating a Key Pair in a Component's NSS DB" on page 159](#)
- c. Export the newly generated certificate from the Manager. See ["Exporting Certificates" on page 162](#)
- d. Delete the expired Manager's certificate from the Console's NSS DB.
- e. Import the Manager's new certificate into the Console's NSS DB. See ["Importing a Certificate into the NSS DB" on page 162](#)

Using the Certificate Revocation List (CRL)

ESM supports the use of CRL to revoke a CA-signed certificate which has been invalidated. The CA that issued the certificates also issues a CRL file which contains a signed list of certificates which it

had previously issued that it now considers invalid. 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 certificate is present in the Manager's `/opt/arcsight/manager/config/jetty/nssdb` directory

In the case of client-side authentication, the Manager validates the authenticity of the client certificate using the certificate of the signing CA.

- You have a current CRL file provided by your CA.

The CA updates the CRL file periodically as and when additional certificates get invalidated.

To use the CRL feature:

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

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

Configuration Required to Support Suite B

Suite B is a set of cryptographic algorithms put forth by the National Security Agency (NSA) as part of the national cryptographic technology. While FIPS 140-2 supports sensitive but unclassified information, FIPS with Suite B supports both unclassified information and most classified up to top secret information. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

When configured to use Suite B mode, ESM supports Suite B Transitional profile. There are 2 level of security defined in Suite B mode:

- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`

Suite B 128-bit security level, providing protection from classified up to secret information

- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`

Suite B 192-bit security level, providing protection from classified up to top secret information

Generating a Key Pair on the Manager

The key pair you generate is used to generate the self-signed certificate. The self-signed certificate automatically gets generated when you generate the key pair.

The Manager's key pair and certificate get generated and stored in its `nssdb`. The Manager's public key is embedded in its certificate, thereby linking the Manager's identity to its public key.

Note: When you import or generate a key pair into `nssdb`, if there is an existing key pair/certificate that has the same Common Name (CN) as the one you create, the `runcertutil` utility uses the alias of the existing key pair for the newly created key pair and ignores the alias you supplied in the `runcertutil` command line.

1. Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory to generate a key pair. This automatically generates the Manager's certificate.

If you want to set the expiry date of the certificate, do so when generating the key pair. After you generate the key pair, you cannot change the expiry date on the certificate.

Caution: Hints on generating a key pair:

- Make sure to use *mykey* as the alias name for the key pair as shown in the example.
- The `-m` serial number should be unique within `nssdb`.
- The hostname is the short name or fully qualified domain name depending upon how your Manager name was set up when you installed the Manager.
- Using `-v` to set the validity period of your certificate is optional. If you do not use this option, the certificate is valid for 3 months by default. If you choose to use it, see ["Setting the Expiration Date of a Certificate" on page 167](#) section in the Administrator's Guide for details.
- The `-q` defines the PQG value with which an ECDSA certificate is generated.

```
./arcsight runcertutil -S -s "CN=<hostname>" -v <number_of_months_the_
certificate_should_be_valid> -n mykey -k ec -q secp521r1 -x -t "C,C,C" -m 1234
-d /opt/arcsight/manager/config/jetty/nssdb
```

(For more information on the `-q secp521r1` option, see ["Types of Key Pairs Used in FIPS Mode" on page 156](#).)

For example, if your hostname is `host.arcsight.com`, you would run:

```
./arcsight runcertutil -S -s "CN=host.arcsight.com" -v 6 -n mykey -k ec -q  
secp521r1 -x -t "C,C,C" -m 1234 -d /opt/arcsight/manager/config/jetty/nssdb
```

Entered the password, when prompted. The default is described in ["NSS database password" on page 47](#).

Enter random keyboard strokes when prompted to generate the random seed used to generate your key.

This generates a key pair and certificate with the alias `mykey` which is valid for 6 months from the current date and time in the Manager's `nssdb`.

2. To check whether the key pair has been successfully created in the `nssdb`, run the following from the Manager's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -d <ARCSIGHT_HOME>/config/jetty/nssdb
```

Exporting the Manager's Certificate

To export the Manager's certificate, run the following command from the Manager's `/opt/arcsight/manager/bin` directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d  
/opt/arcsight/manager/config/jetty/nssdb -o <absolute_path_to _  
managercertificatename.cert>
```

Note: The `-o` specifies the absolute path to where you want to place the exported Manager's certificate. If you do not specify the absolute path the file is exported to your `/opt/arcsight/manager` directory by default.

For example, to export the certificate as a file named `ManagerCert.cer` to `/opt/arcsight/manager` directory, run:

```
./arcsight runcertutil -L -n mykey -r -d /opt/arcsight/manager/config/jetty/nssdb -  
o /opt/arcsight/manager/ManagerCert.cer
```

This generates the `ManagerCert.cer` file, the Manager's certificate, in the `/opt/arcsight/manager` directory.

Importing a Certificate into the Manager

Import a certificate into the Manager:

```
./arcsight runcertutil -A -n <certificate_name> -t "CT,C,C" -d  
/opt/arcsight/manager/config/jetty/nssdb -i <absolute_path_to_the_root_certificate>
```

For the `-t` option, be sure to use `CT,C,C` permissions flags only and in the same order that it is shown above.

Changing a Default Mode Installation to FIPS 140-2

Caution: Before migrating from default mode to FIPS mode, keep in mind that pre-v4.0 Loggers cannot communicate with a FIPS-enabled Manager.

- If you are converting to FIPS, convert all components to FIPS.
- We do not support Default to Suite B conversion in this release.

To convert an existing default mode installation to FIPS mode, on each component, migrate the existing certificates and key pairs from the component's cacerts and keystore to the component's NSSDB. The following sub-sections provide you step-by-step instructions on how to do so for each component.

Manager

You can use `keytool` to for the task described below. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

To convert an existing Manager from default mode to FIPS mode you will export the certificate and import the key pair. Then you will run commands from the Manager's bin directory to verify the key pair import and import the certificate.

To use the `keytoolgui`, export the certificate, and import the key pair:

1. Log in as user *arcsight*.

2. Stop the Manager if it is running.

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

3. Export the Manager's key pair from the Manager's
`/opt/arcsight/manager/config/jetty/keystore`.

- a. Start the `keytoolgui` by running the following from the Manager's `/bin` directory:
`./arcsight keytoolgui`
- b. Click **File->Open KeyStore** and navigate to the Manager's
`/opt/arcsight/manager/config/jetty/keystore`.

- c. When prompted, enter the password that you set for the keystore. For the default, see ["Keystore password" on page 46](#).
 - d. Right-click the key pair and select **Export**.
 - e. Select **Private Key and Certificates** radio button and click **OK**.
 - f. Enter the password for the key pair when prompted and click **OK**.
 - g. Enter the new password for the keypair being exported and click **OK**.
 - h. Navigate to the location on your machine to where you want to export the key pair.
 - i. Enter `mykey.pfx` as the name for the key pair (make sure to use a `.pfx` extension) in the Filename textbox and click **Export**.
 - j. An `Export Successful` message appears. Click **OK**.
 - k. Select **File > Exit** to exit `keytoolgui`.
4. Import the Manager's key pair that you had exported in Step 3 into the Manager's `nssdb`. To do so, run the following command from the Manager's `bin` directory:
- ```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
/opt/arcsight/manager/config/jetty/nssdb
```
- Enter the password for the Manager's `nssdb` when prompted. The default is described in ["NSS database password" on page 47](#).
- Enter the password for the `.pfx` key pair file that you are importing. This is the password that you set in substep **g**, of Step 3, in this procedure.
5. Run the following command from your Manager's `bin` directory to verify that the key pair is imported correctly. The alias of the key pair imported in the `nssdb` is `mykey`.
- ```
./arcsight runcertutil -L -d <ARCSIGHT_HOME>/config/jetty/nssdb
```
6. Run the Manager setup program from the Manager's `/bin` directory:
- ```
./arcsight managersetup
```
7. Select **Run Manager in FIPS mode**.
8. Follow the prompts in the next few screens until the wizard informs you that you have successfully configured the Manager.
9. Restart the Manager.

## ArcSight Console

For ArcSight Console on 64-bit Linux 6.1, install the 32-bit zlib package to make sure that you do not encounter errors when enabling and disabling FIPS mode using `runmodutil`.

You can use `keytool` to for the task described below. Use of `keytool` (which runs from the command line in a terminal window) is preferred. Using the `keytoolgui` interface requires that the X Window system be installed on your system. Note that using the X Window system is not preferred, but if you have it installed and want to use it, you can use `keytoolgui`. The X Window system is not present on the ESM Express appliance.

To convert an existing ArcSight Console from default mode to FIPS mode, migrate the Manager's certificates from the Console's `<ARCSIGHT_HOME>\current\jre\lib\security\cacerts` into the Console's `nssdb.client` as described in the procedure below:

1. Stop the ArcSight Console if it is running.
2. Export the existing Manager certificate. To export the Manager's certificate, run the following command from the Manager's `/opt/arcsight/manager/bin` directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -
/opt/arcsight/manager/config/jetty/nssdb -o <absolute_path_to_
managercertificatename.cert>
```

**Note:** If you do not specify the `-o` absolute path option, the file is exported to your `<ARCSIGHT_HOME>` directory by default.

3. Run the following command from the Console's `<ARCSIGHT_HOME>\current\bin` directory to import the certificate(s) you just exported in the above steps into the Console's `<ARCSIGHT_HOME>\current\config\nssdb.client`. If you are importing multiple certificates, you import them one at a time.

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t "CT,C,C" -d
<ARCSIGHT_HOME>\current\config\nssdb.client -i <absolute_path_to_certificate's
name>.cer>
```

4. If you have client-side authentication configured, export the Console's key pair and certificate from the Console's `<ARCSIGHT_HOME>\current\config\keystore.client` using `keytoolgui`. Make sure to export the key pair in `.pfx` format.
  - a. Start the `keytoolgui` by running the following from the Console's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight keytoolgui
```
  - b. Click **File->Open KeyStore** and navigate to the Console's `<ARCSIGHT_HOME>/config/jetty/keystore`.

- c. When prompted, enter the password that you set for the keystore. For the default password, see ["Keystore password" on page 46](#).
- d. Right-click the key pair and select **Export**.
- e. Select **Private Key and Certificates** radio button and click **OK**.
- f. Enter the password for the key pair when prompted and click **OK**. The default should be the same as the keystore.
- g. Navigate to the location on your machine to where you want to export the key pair.
- h. Enter `mykey.pfx` as the name for the key pair (make sure to use a `.pfx` extension) in the Filename textbox and click **Export**.
- i. An Export Successful message appears. Click **OK**.
- j. Import the key pair you just exported into the Console by running the following command from the ArcSight Console's `\bin` directory:

```
arcsight runpk12util -i <your_file_name.pfx> -d <ARCSIGHT_HOME>\current\config\nssdb.client
```

- k. Export the Console's certificate. See the section ["Exporting Certificates" on page 162](#) ("From the Console" subsection) for detailed instructions.
- l. Stop the Manager if it is running.
- m. Import the Console's certificate into the Manager's `nssdb`. See the section ["Importing a Certificate into the NSS DB" on page 162](#) ("On the Manager" subsection) for details.

**Caution:** Make sure that you do NOT use the alias `mykey` for the certificate when importing it into the Manager's `nssdb` because the `nssdb` already has the Manager's certificate with the alias `mykey` in it. All aliases in the `nssdb` must be unique.

- n. Start the Manager.
5. Run the Console's setup program by running the following from the Console's `\bin` directory:
- ```
arcsight consolesetup
```
6. Select **No, I do not want to transfer the settings**.
7. Select **Run Console in FIPS mode**.
8. It asks you to confirm that you have configured the NSS DB. Click **Yes**. You see another message telling you that you cannot convert back to default mode. Click **Yes**.

9. Follow the prompts in the next few screens until the wizard informs you that you have successfully configured the Console. Refer to the ESM Installation and Configuration Guide, if you need more information on the wizard for installing the ArcSight Console.

When you start the Console, you should see a message in the `/logs/console.log` file telling you that the Console has started in FIPS mode.

10. Set your browser to use FIPS. See ["Configure Your Browser for FIPS " below](#).

Connectors

For information on configuring Connectors for FIPS, refer to SmartConnector Configuration Guide for each SmartConnector.

Configure Your Browser for FIPS

To connect a browser to a FIPS web server, the browser must be configured to support FIPS. Review the documentation for your browser and follow the instructions to make it FIPS compliant before using it for ArcSight Console online help or to connect to the ArcSight Command Center.

Make sure that all SSL protocols are turned off. For example, on Microsoft Internet Explorer (IE):

1. Select **Tools > Internet Options**.
2. Select the **Advanced** tab.
3. Scroll down to the **Security** section.
4. Uncheck **Use SSL 2.0** and **Use SSL 3.0**.
5. Check the TLS options. By default ESM uses TLS 1.0.

Other browsers (and other versions of IE) may have different menu items or options for doing this, so refer to your browser documentation.

When using a browser with Suite B, it matters how you generate your key pair. For information about the encryption to use with browsers, see ["Types of Key Pairs Used in FIPS Mode" on page 156](#).

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Administrator's Guide (ESM 6.9.0c)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!