

Administrator's Guide

ArcSight ESM 5.5

April 22, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

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

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

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

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

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

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWl .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
04/22/2013	ArcSight ESM Version 5.5	new features

Contents

Chapter 1: Basic Administration Tasks	9
Starting Components	9
Starting the ArcSight Manager	9
Decoupled Process Execution	10
Stopping the ArcSight Manager	10
Starting the ArcSight Console	10
Reconnecting ArcSight Console to the Manager	10
Starting ArcSight Web	11
Starting ArcSight SmartConnectors	11
Starting Connector Management Services	11
Configuring ArcSight Manager or ArcSight Web as a Service	11
ArcSight Manager Service Setup on Windows	12
Starting and Stopping the ArcSight Manager Service on Windows	12
Removing the ArcSight Manager Service on Windows	12
ArcSight Manager or ArcSight Web Service Setup on Unix Platforms	12
Reducing Impact of Anti-Virus Scanning	13
License Tracking and Auditing	13
ArcSight System Tasks	14
Setting up a Custom Login Banner and Logo	14
Setting up a Custom Login Banner	14
Setting up Custom Logo for ArcSight Web	15
Chapter 2: Configuration	17
Managing and Changing Properties File Settings	17
Property File Format	17
Defaults and User Properties	18
Editing Properties Files	18
Dynamic Properties	19
Example	20
Changing Manager Properties Dynamically	21
Changing the Service Layer Container Port	22
Securing the Manager Properties File	22
Adjusting Console Memory	23
Adjusting Pattern Discovery Memory	23

Installing New License Files Obtained from HP	24
Installing in Silent Mode	24
Configuring Manager Logging	24
Sending logs and diagnostics to HP Support	25
Guidelines for using the Send Logs utility	26
Gathering logs and diagnostic information	26
Understanding SSL Authentication	33
Terminology	34
Tools for SSL Configuration	38
Keytoolgui	38
keytool	43
tempca	44
How SSL Works	44
SSL certificates	45
Types	45
Comparing Self-signed and CA-signed certificates	46
Viewing Certificate Information	46
Using a Demo Certificate	46
Using a Self-Signed Certificate	47
When clients communicate with one Manager	47
When clients communicate with multiple Managers	50
Using a CA-Signed SSL Certificate	51
Create a Key Pair for a CA-Signed Certificate	52
Send for the CA-Signed Certificate	53
Import the CA Root Certificate	53
Import the CA-Signed Certificate	53
Restart the Manager	56
Accommodating Additional Components	57
Removing a Demo Certificate	57
Replacing an Expired Certificate	57
Establishing SSL Client Authentication	58
Setting up SSL Client-Side Authentication on ArcSight Console	58
Setting up SSL Client Authentication on ArcSight Web	65
Setting up Client-side Authentication on Partition Archiver and SmartConnectors	70
Migrating from one certificate type to another	72
Migrating from Demo to Self-Signed	72
Migrating from Demo to CA-Signed	72
Migrating from Self-Signed to CA-Signed	73
Verifying SSL Certificate Use	73
Sample output for verifying SSL certificate use	73
Using Certificates to Authenticate Users to ArcSight	74
Using the Certificate Revocation List (CRL)	74
Reconfiguring the ArcSight Console after Installation	75

Reconfiguring ArcSight Manager	75
Changing ArcSight Manager Ports	75
Changing ArcSight Web Session Timeouts	76
Managing Password Configuration	76
Enforcing Good Password Selection	76
Password Length	76
Restricting Passwords Containing User Name	76
Password Character Sets	77
Requiring Mix of Characters in Passwords	77
Checking Passwords with Regular Expressions	78
Password Uniqueness	79
Setting Password Expiration	79
Restricting the Number of Failed Log Ins	79
Disabling Inactive User Accounts	80
Re-Enabling User Accounts	80
Properties Related to Domain Field Sets	80
Advanced Configuration for Asset Auto-Creation	81
Asset Auto-Creation from Scanners in Dynamic Zones	81
Create Asset with either IP Address or Host Name	82
Preserve Previous Assets	83
Changing the Default Naming Scheme	84
Compression and Turbo Modes	84
Compressing SmartConnector Events	84
Reducing Event Fields with Turbo Modes	84
Turbo Mode and Domain Fields	86
Configuring the ArcSight Database Monitor	86
Configuring Database Monitor e-mail message recipients	86
Configuring the check for free space in Oracle tablespaces	87
Sending Events as SNMP Traps	87
Configuration of the SNMP trap sender	87
Asset Aging	89
Excluding Assets From Aging	89
Task to Disable Assets of a Certain Age	89
To Delete an Asset	89
Amortize Model confidence with scanned asset age	90
Configuring Actors	90
Tuning Guide for Supporting Large Actor Models	92
Permissions Required to Use Actor-Related Data	93
About Exporting Actors	94
Chapter 3: Running the Manager Configuration Wizard	95
Running the Wizard	95
Authentication Details	101

How external authentication works	101
Guidelines for setting up external authentication	101
Password Based Authentication	102
Password Based and SSL Client Based Authentication	105
Password Based or SSL Client Based Authentication	105
SSL Client Only Authentication	105
Chapter 4: Database Administration	107
Changing Oracle Initialization Parameters	107
Monitoring Available Free Space in Tablespaces	108
Setting Up Database Threshold Notification	108
Resetting the Oracle Password	109
Backing up ArcSight Databases	109
Oracle Cold Backup	109
Oracle Hot Backup	109
Exporting Data	110
Recovering ArcSight Databases	110
Speeding up partition compression	110
Partition logs	111
Chapter 5: Managing Resources	113
Appendix A: Administrative Commands	115
ArcSight Commands	115
Archive Command Details	123
Remote Mode	123
Standalone Mode	124
Exporting Resources to an Archive	124
Importing Resources from an Archive	125
Syntax for Performing Common Archive Tasks	125
Appendix B: Troubleshooting	161
General	161
Scheduled Rules Take too Long or Time Out	162
Query and Trend Performance Tuning	164
Persistent Database Hints	164
server.defaults.properties Entries for Trends	164
Troubleshooting Checklist after Restarting the Manager	165
Disable these Trends on High Throughput Systems	165
How do you know when a trend is caught up?	166
How long does it take a trend to catch up?	166
Enhancing the Performance Globally for all Database Queries	166
Unable to Execute Query: ORA-01555	167
SmartConnectors	167

ArcSight Console	168
Manager	170
Manager shuts down.	170
ArcSight Web	171
Database	172
SSL	173
Cannot connect to the SSL server: IO Exception in the server logs	173
Cannot connect to the SSL server	173
PKIX exchange failed/could not establish trust chain	173
Issuer certificate expired	173
Cannot connect to the Manager: Exception in the server log	174
Certificate is invalid	174
Issue with Internet Explorer and ArcSight Web in FIPS Mode	174
Appendix C: Monitoring Database Attributes	177
Understanding Database Checks	177
Message text	177
Disabling Database Checks	178
List of Database Check Tasks	179
Appendix D: The Logfu Utility	183
Running Logfu	184
Example	186
Troubleshooting	186
Menu	188
Typical Data Attributes	188
Intervals	189
Appendix E: Creating Custom E-mails Using Velocity Templates	191
Overview	191
Notification Velocity templates	191
Commonly used elements in Email.vm and Informative.vm files	191
The #if statement	192
Contents of Email.vm and Informative.vm	192
Using Email.vm and Informative.vm Template Files	193
Understanding the Customization Process	193
Customizing the template files	194
Sample Output	195
Appendix F: Configuration Changes Related to FIPS	197
Tools Used to Configure Components in FIPS	198
FIPS Encryption	198
Types of Certificates Used in FIPS Mode	199

Using a Self-Signed Certificate	199
Using a Certificate Authority (CA) Signed Certificate	199
Steps Performed on the Manager	199
Steps Performed on ArcSight Web	203
Steps Performed on the ArcSight Console	207
Some Often-Used SSL-Related Procedures	207
Generating a Key Pair in a Component's NSS DB	207
On the Manager	207
On ArcSight Web	208
Verifying Whether the Key pair Has Been Successfully Created	209
Viewing the Contents of the Manager Certificate	209
Exporting Certificates	209
Exporting a Certificate From the Manager	209
Exporting a Certificate From the Console	209
Exporting a Certificate From the Web	210
Importing a Certificate into the NSS DB	210
On the Manager	210
On the Console	210
On ArcSight Web	211
Importing an Existing Key Pair into the NSS DB	211
Setting up Server-Side Authentication	212
Setting up Client-Side Authentication	212
Changing the Password for NSS DB	213
Listing the Contents of the NSS DB	214
Viewing the Contents of a Certificate	215
Setting the Expiration Date of a Certificate	215
Deleting a Certificate from NSS DB	215
Replacing an Expired Certificate	215
Using the Certificate Revocation List (CRL)	216
Configuration Required to Support Suite B	217
Generating a Keypair on the Manager	217
Exporting the Manager's Certificate	218
Importing a Certificate into the Manager	218
Changing a Default Mode Installation to FIPS 140-2	219
Manager	219
ArcSight Console	221
ArcSight Web	222
Configure Your Browser for FIPS	224
FIPS with Firefox	224
Partition Archiver	227
Index	229

Chapter 1

Basic Administration Tasks

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

The following topics are covered here:

- [“Starting Components” on page 9](#)
- [“Configuring ArcSight Manager or ArcSight Web as a Service” on page 11](#)
- [“Reducing Impact of Anti-Virus Scanning” on page 13](#)
- [“License Tracking and Auditing” on page 13](#)
- [“ArcSight System Tasks” on page 14](#)
- [“Setting up a Custom Login Banner and Logo” on page 14](#)

Starting Components

Unless ESM is configured to run as a service, you run the Manager, Console, and SmartConnectors using the Start menu. For Unix systems, you need to 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 you can use to start up, shut down, configure, or reconfigure ESM components. In addition, it provides information about setting up the Manager as a daemon (on Unix platforms) or as a service (on Windows), if you didn't originally configure the Manager that way.

Starting the ArcSight Manager

To start the Manager from the command line, if it's not configured to run either as a daemon or a service: Start the Manager by running the following command as user *arcsight*:

```
/sbin/service arcsight_services start manager
```

When it starts, the Manager displays a stream of messages in the command window or terminal box to reflect its status. The command window displays the word “Ready” when the Manager has started successfully. When you start the Manager as a service, to monitor whether it has successfully loaded, view the `server.std.log` file, located in `<ARCSIGHT_HOME>\logs\default` on Windows. On Unix systems, use the command:

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

On Windows systems, you can use a “tail” equivalent tool to run the same command, such as those available from <http://www.cygwin.com>, which provides Unix environments and tools for Windows.

Decoupled Process Execution

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

The process executor is used, by default, on all Unix platforms. The 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, in the same fashion as the Manager, so if the process stops for any reason, it restarts automatically. The process executor is transparent to users regarding the way that the Manager is started or stopped.

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

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

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

Stopping the ArcSight Manager

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

Starting the ArcSight Console

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

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

```
./arcsight console
```

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**.



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

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

Starting ArcSight Web

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

Starting ArcSight SmartConnectors

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

To start up an ArcSight SmartConnector:

- 1 Open a command window or terminal box and navigate to the connector's `/current/bin` directory.
- 2 Type in the following line and press **Enter**:

```
./arcsight agents
```

The connector in that folder starts.

Starting Connector Management Services

To start the Connector Management Service run the following command as user *arcsight*:

```
/sbin/service arcsight_services start conapp
```

To start the service for a connector container run the following command as user *root*:

```
/sbin/service arcsight_services start connector_<N>
```

...where *<N>* is the number of the container whose service you want to start.

Configuring ArcSight Manager or ArcSight Web as a Service

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

ArcSight Manager Service Setup on Windows

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

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

```
arcsight managersvc -i
```

On a 64-bit machine enter:

```
arcsight managersvc64 -i
```

Starting and Stopping the ArcSight Manager Service on Windows

To start or stop the Manager service:

- 1 Right-click the **My Computer** icon, and select **Manage**. The Computer Management window appears.
- 2 Within the Computer Management window, expand the Services and Applications folder.
- 3 Click **Services**.
- 4 Right-click the Manager service name and select **Start to begin the service** or **Stop to end the service**

Removing the ArcSight Manager Service on Windows

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

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

```
arcsight managersvc -r
```

On 64-bit machine enter:

```
arcsight managersvc64 -r
```

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

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

ArcSight Manager or ArcSight Web Service Setup on Unix Platforms

The following provides a brief overview of how to set up the Manager or ArcSight Web as a daemon, the “service” equivalent on Unix platform machines. After installation, the Manager can be controlled using `/etc/init.d/arcsight_manager start|stop`, (or `arcsight_web` for ArcSight Web) following the standard method of starting daemon services in Unix. Change the configuration file `/etc/arcsight/arcsight_manager.conf` (or `arcsight_web.conf` for ArcSight

Web) to reflect the installation directory and other settings. In addition, the `/etc/init.d/arcsight_*` scripts are hooked into the Unix startup procedure, making the Manager or Web start and shut down in lock step with the host OS.

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

```
./arcsight managersetup
./arcsight websetup
```

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

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



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

Reducing Impact of Anti-Virus Scanning

Files in certain 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`

License Tracking and Auditing

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

ArcSight System Tasks

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

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

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

Event Partition Statistics Updater: This task updates statistics on the partitioned event tables, acting on today's partition.

Partition Archiver: This task archives event partitions based on your retention policy.

Partition Compressor: This task compresses event partitions based on your retention policy.

Partition Manager: This task creates/drops partitions based on your retention policy.

For information on the partition-related tasks refer to the “Configuring Partition Management” topic in the “Installing ArcSight Database” chapter of the ESM Installation and Configuration Guide.

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 in sync, based on the current indices in the database.

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

Setting up a Custom Login Banner and Logo

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

You can configure the ArcSight Web server so that ArcSight Web displays a customized logo or other image.

Setting up a Custom Login Banner

You can create a custom message that the ArcSight Console or ArcSight Web displays before users log in. 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 or ArcSight Web. (Changes to the properties file take effect the next time the Manager is started.)

Create a text file named `loginbanner.txt` in the `<ARCSIGHT_HOME>/config` directory. This feature is often used to display a legal disclaimer message. Users must close the message window before they can log in. The ArcSight Web console displays the custom banner as well, provided that the browser used supports JavaScript and has JavaScript enabled.

Setting up Custom Logo for ArcSight Web

To configure a custom logo for ArcSight Web:

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

```
# logo image for login page
```

```
loginLogoImg = <demo-logo-login.png>
```

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

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



Caution

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

Chapter 2

Configuration

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

- [“Managing and Changing Properties File Settings” on page 17](#)
- [“Adjusting Console Memory” on page 23](#)
- [“Adjusting Pattern Discovery Memory” on page 23](#)
- [“Installing New License Files Obtained from HP” on page 24](#)
- [“Configuring Manager Logging” on page 24](#)
- [“Understanding SSL Authentication” on page 33](#)
- [“Reconfiguring the ArcSight Console after Installation” on page 75](#)
- [“Reconfiguring ArcSight Manager” on page 75](#)
- [“Managing Password Configuration” on page 76](#)
- [“Properties Related to Domain Field Sets” on page 80](#)
- [“Advanced Configuration for Asset Auto-Creation” on page 81](#)
- [“Compression and Turbo Modes” on page 84](#)
- [“Sending Events as SNMP Traps” on page 87](#)
- [“Asset Aging” on page 89](#)
- [“Configuring Actors” on page 90](#)

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

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

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

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

Defaults and User Properties

Most configuration items in various components consist of at least two files. The first, is the defaults properties file, such as `server.defaults.properties`. It contains the default settings. You should not modify these files; use them as a reference.

The second file, is the user properties file, such as `server.properties`. It can contain any properties from the defaults properties file, but the property values in this file override those in the defaults file. Thus, it contains settings that are specific to a particular installation. Typically, the user properties file for a component is created and modified automatically when you configure the component using its configuration wizard.

Because the user properties file contains settings you specify to suit your environment, it is never replaced by an upgrade. If an upgrade, such as a service pack or a version update, changes any properties, it does so in the defaults file.

The following table lists the most important properties files.

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

Editing Properties Files

When you edit a `*.properties` file, first look for the `*.defaults.properties` file. Copy the property you want to edit from `*.defaults.properties` to `*.properties` and change the setting to your new value in `*.properties`. When the same property is defined differently in each file, the system uses the value in `*.properties`. This ensures that when you install an upgrade, and the `*.defaults.properties` file is updated, the properties you customized are retained unchanged in `*.properties`.

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

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

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

If you change a communication port, be sure to change both sides of the connection. For example, if you configure a Manager to listen to a different port than 8443, be sure to

configure all the Manager's clients (Consoles, SmartConnectors, ArcSight Web, and so on) to use the new port as well.

Protocol	Port	Configuration
ICMP	none	ArcSight Console to Target communication (ping tool)
UDP	1645 or 1812	Manager to RADIUS server (if enabled)
TCP	9443	ArcSight Web
	9090	ESM Service Layer Container Port
TCP	8443	Management Console and ArcSight Console to Manager communication
TCP	8443	SmartConnector to Manager communication
TCP	1521	Manager to ArcSight Database (Oracle communication)
TCP	636	Manager to LDAP server (w/ SSL if enabled)*
TCP	389	Manager to LDAP server (w/o SSL if enabled)*
TCP	143	Manager to IMAP server (for Notifications)
TCP	110	Manager to POP3 server (for Notifications)
UDP/TCP	53	ArcSight Console to DNS Server communication (nslookup tool)
UDP/TCP	43	ArcSight Console to Whois Server communication (whois tool)
TCP	25	Manager to SMTP server (for Notifications)

Dynamic Properties

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

- `auth.auto.reenable.time`
- `auth.enforce.single.sessions.console`
- `auth.enforce.single.sessions.web`
- `auth.failed.max`
- `auth.password.age`
- `auth.password.age.exclude`
- `auth.password.different.min`
- `auth.password.length.max`
- `auth.password.length.min`
- `auth.password.letters.max`
- `auth.password.letters.min`
- `auth.password.maxconsecutive`
- `auth.password.maxoldsubstring`

- `auth.password.numbers.max`
- `auth.password.numbers.min`
- `auth.password.others.max`
- `auth.password.others.min`
- `auth.password.regex.match`
- `auth.password.regex.reject`
- `auth.password.unique`
- `auth.password.userid.allowed`
- `auth.password.whitespace.max`
- `auth.password.whitespace.min`
- `external.export.interval`
- `process.execute.direct`
- `servletcontainer.jetty311.log`
- `servletcontainer.jetty311.socket.https.expirationwarn.days`
- `ssl.debug`
- `web.accept.ips`
- `whine.notify.emails`
- `xmlrpc.accept.ips`

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

Example

Manager M1 starts successfully for the first time on September 26, 2012, 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.2012_09_26_14_45_27_718
```

On September 27, 2010, the M1 administrator adds the following property to the `server.properties` file:

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

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

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

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

```
server.properties.2012_09_26_14_45_27_718
```

```
server.properties.2012_09_27_01_05_40_615
```

On September 28, 2012, the M1 administrator adds this property to the `server.properties` file:

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

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

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

```
server.properties.2012_09_26_14_45_27_718
```

```
server.properties.2012_09_27_01_05_40_615
```

```
server.properties.2012_09_28_03_25_45_312
```

On September 29, 2012, the M1 administrator updates the `whine.notify.emails` property in the `server.properties` file. When he runs the `manager-reload-config` command, the command fails because this property cannot be loaded dynamically. As a result, these things happen:

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

```
server.properties.2012_09_26_14_45_27_718
```

```
server.properties.2012_09_27_01_05_40_615
```

```
server.properties.2012_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 [Appendix A, Administrative Commands](#), on page 115.

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

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

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

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

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

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

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



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

Changing the Service Layer Container Port

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

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

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

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

- 2 Restart the Manager.

Securing the 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. As a result, the `server.properties` file must be protected 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.



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

Adjusting Console Memory

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

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

Adjusting Pattern Discovery Memory

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

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

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

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

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

Installing New License Files Obtained from HP

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

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

```
./arcsight deploylicense
```
- 3 Restart the Manager.

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

Installing in Silent Mode

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

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

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

```
LicenseChoice=1  
  
LicenseFile.filename=<name_of_the_license_zip_file>  
  
replaceLicenseQuestion =yes
```
- 5 Save this text file as `properties.txt` in the Manager's <ARCSIGHT_HOME>.
- 6 From the Manager's bin directory, run:

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

Configuring Manager Logging

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

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

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

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

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

```
# Maximum size of a log file.

log.channel.file.property.maxsize=10MB

# Maximum number of roll over files.

log.channel.file.property.maxbackupindex=10
```

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

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

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

Sending logs and diagnostics to HP Support

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

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



Note

You can also use the `arcldt` command to run specific diagnostic utilities from the Manager command line. For more information, see [Appendix A, Administrative Commands](#), on page 115.

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

Guidelines for using the Send Logs utility

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

- You can be connected as any valid user on an ESM component to collect its local logs; however, you must have administrator access to collect logs from other components. For example, if you are connected as user 'joe' to the Console, you can collect its logs. But if you need to collect logs for the Manager and the database, you must connect to the Console as the administrator.
- SmartConnectors must be running version 4037 or later to remotely (using a Console or the Manager) collect logs from them.
- You can only collect local logs on SmartConnectors or the ArcSight Database. The Send Logs utility only collects logs for the component on which you run it.
- You can run the Send Logs utility on a component that is down. That is, if the Database is down, you can still collect its logs using this utility.

If the Manager is down, you can only collect its local logs. However, if you need to collect the database logs as well, use the `arcctl` command on the Manager. For more information, see [Appendix A, Administrative Commands, on page 115](#).

- All log files for a component are gathered and compressed. That is, you cannot select a subset of log files that the utility should process.
- The Send Logs utility generates a compressed file on your local system that you can send to Customer Support by e-mail, if they request it.
- You can review the compressed file to ensure that only a desired and appropriate amount of information is sent to support.
- You can remove or sanitize information such as IP addresses, host names, and e-mail addresses from the log files before compressing them. The options are:

- ◆ Send log as generated

This option, the default, does not remove any information from the logs files.

- ◆ Only remove IP address

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

- ◆ Remove IP address, host names, e-mail addresses

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

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

Gathering logs and diagnostic information

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

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

```
./arcsight agent sendlogs
```

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

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

```
./arcsight sendlogs
```

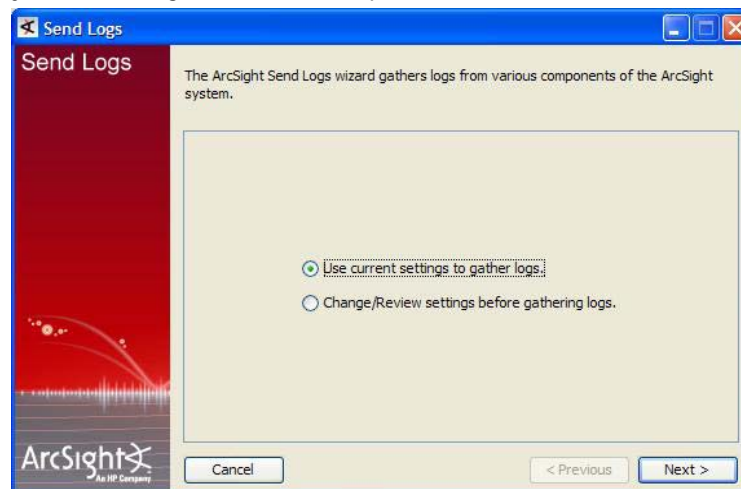
The above action starts the Send Logs wizard. In the wizard screens, perform these steps:



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.

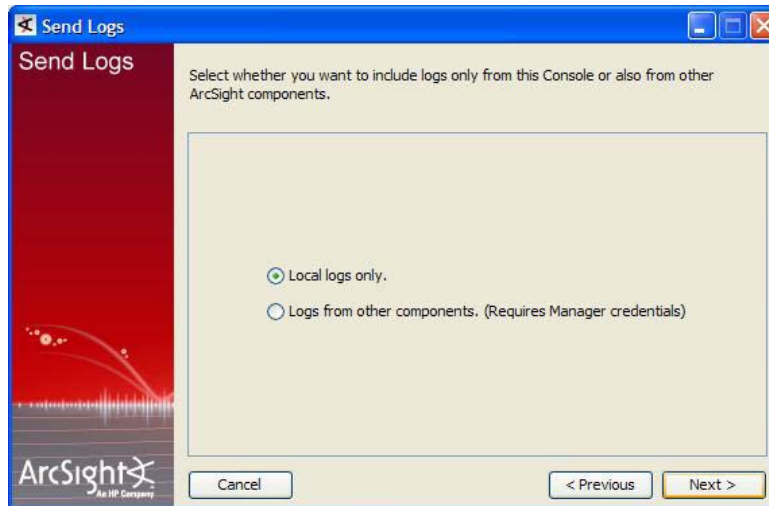


If you select **Use current settings to gather logs**, logs for all components are gathered thus: If this is the first sendlogs is run after installation, then all the logs are gathered. If this is not the first sendlogs is run, then it uses the same setting as the previous run.

- a Enter the Manager's login information.
- b Go to [Step 2 on page 31](#).

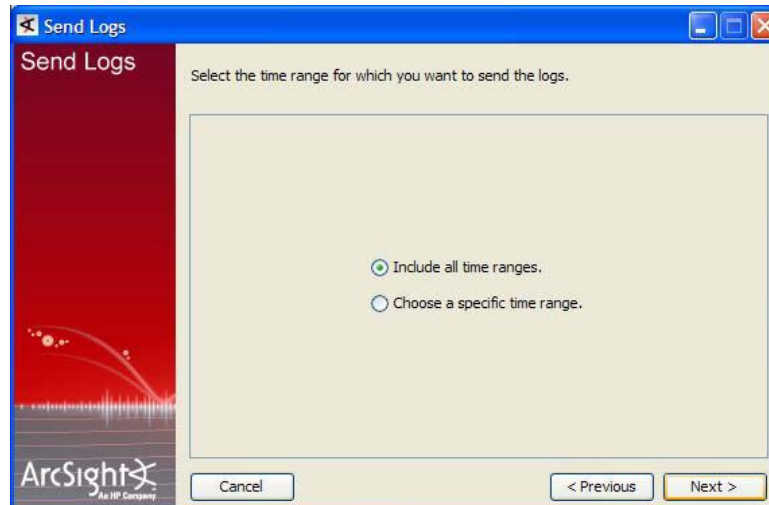
If you selected **Change/Review settings before gathering logs**., you get the option to select the components for which you want logs gathered.

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



Local logs only:

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



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

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

The 'Send Logs' dialog box has a red sidebar with the ArcSight logo. The main area has a light beige background. At the top, it says 'Please specify a time range. Only log entries within this time range will be included.' Below this, there are two rows of date and time pickers. The first row is labeled 'Start Time' and shows '12 Sep 2012 12:18:19 PDT'. The second row is labeled 'End Time' and shows '19 Sep 2012 12:18:19 PDT'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

Logs from other components (Requires Manager credentials):

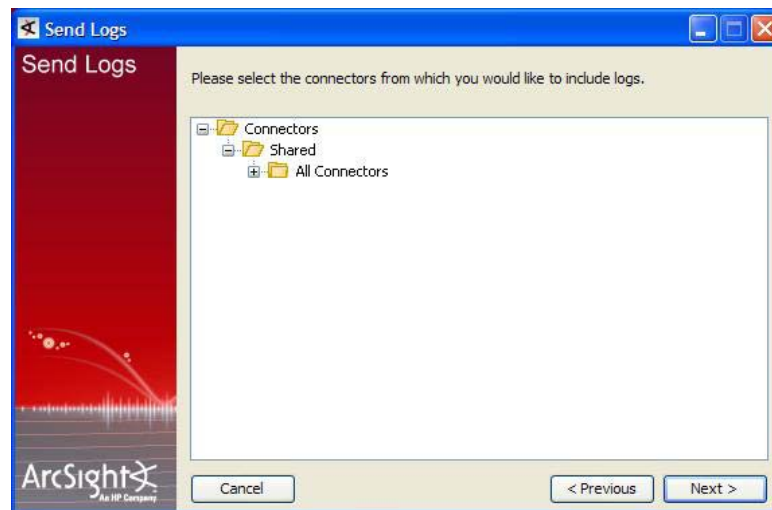
If you select **Logs from other components (Requires Manager credentials)**, you are prompted to choose the components.

- a Select the components and the time range for which you want to gather logs. In addition, select whether you want to run the diagnostic utilities to gather additional information for those components. (The options below might be labeled differently for different versions of this product. For example “CORR-Engine” is “Database” in ESM with Oracle.)

The 'Send Logs' dialog box has a red sidebar with the ArcSight logo. The main area has a light beige background. At the top, it says 'Choose the components for which you want to gather logs and diagnostic information.' Below this, there are five rows of dropdown menus. The first row is labeled 'Manager' and shows 'Yes'. The second row is labeled 'Connectors' and shows 'No'. The third row is labeled 'CORR Engine' and shows 'Yes'. The fourth row is labeled 'Diagnostics' and shows 'Run default set of diagnostic tools'. The fifth row is labeled 'Time range' and shows 'Include all time ranges'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

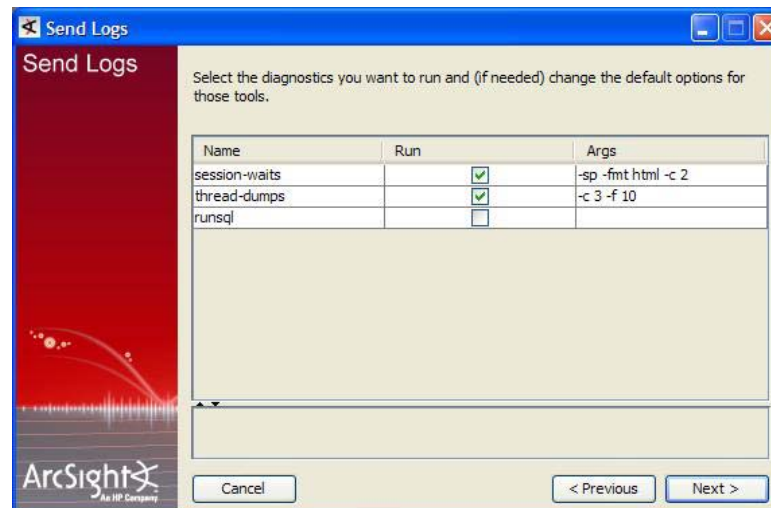
If you choose to specify the diagnostic utilities to run, you are prompted to select the utilities from a list in a later screen. The diagnostic utilities you can select are described in [Appendix A, arcdt, on page 119](#).

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



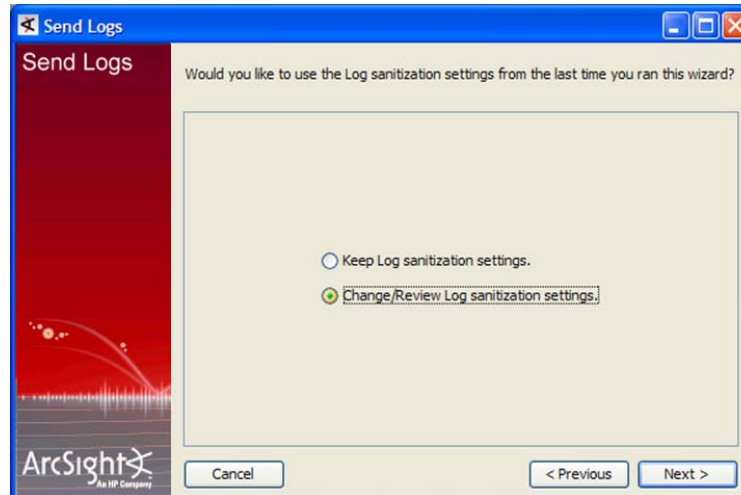
At a minimum, the SmartConnectors should be running version 4037 or later.

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



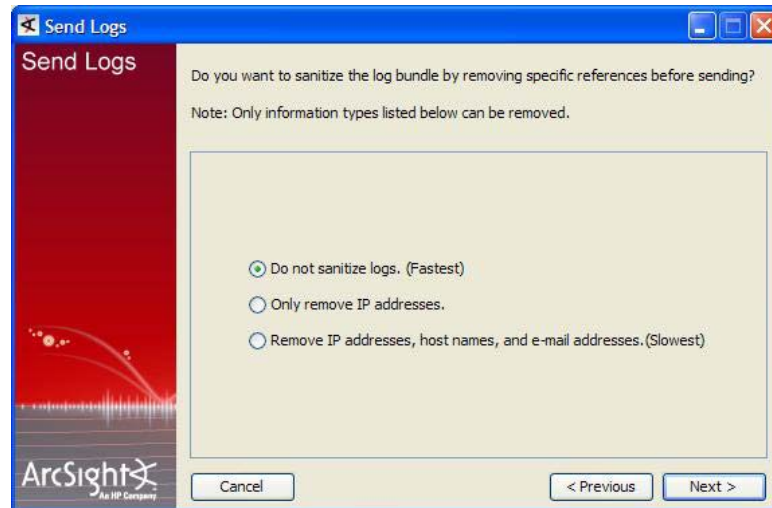
- d Go to [Step 2 on page 31](#).

- 2 Select whether you want to sanitize the logs before collecting them. For more information about sanitizing options, see ["Guidelines for using the Send Logs utility" on page 26.](#)



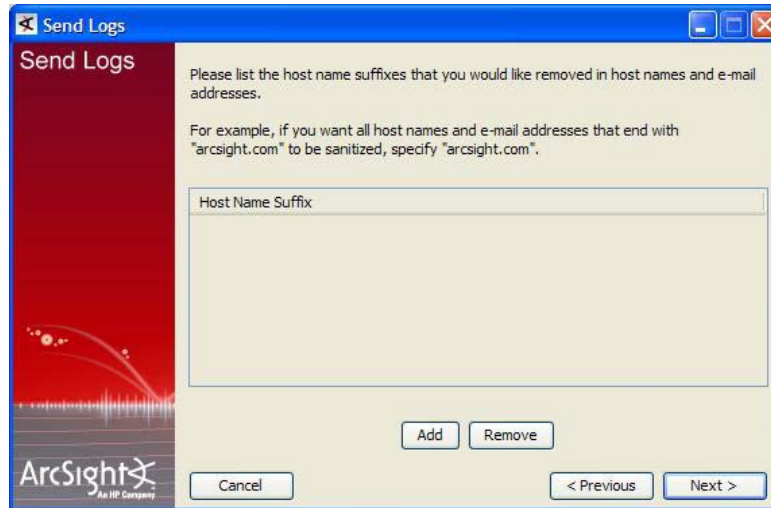
If you choose **Keep Log sanitization settings**, go to [Step 3 on page 32.](#)

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



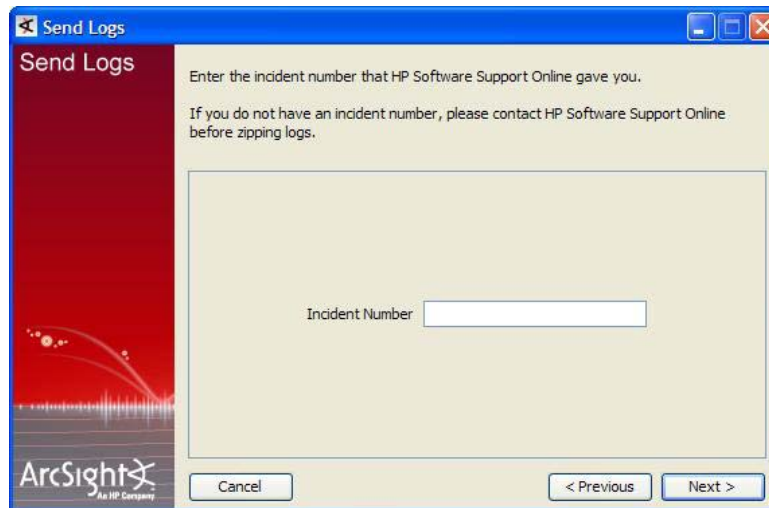
If you chose one of the first two options, go to [Step 3 on page 32.](#)

If you selected **Remove IP addresses, host names, and e-mail addresses (Slower)**, 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.



The 'Send Logs' dialog box has a blue title bar and a red sidebar with the ArcSight logo. The main area is white and contains the following text: 'Please list the host name suffixes that you would like removed in host names and e-mail addresses.' and 'For example, if you want all host names and e-mail addresses that end with "arcsight.com" to be sanitized, specify "arcsight.com".' Below this is a large text input field labeled 'Host Name Suffix'. At the bottom are four buttons: 'Add', 'Remove', 'Cancel', and '< Previous' and 'Next >'.

3 Enter the Customer Support incident number.

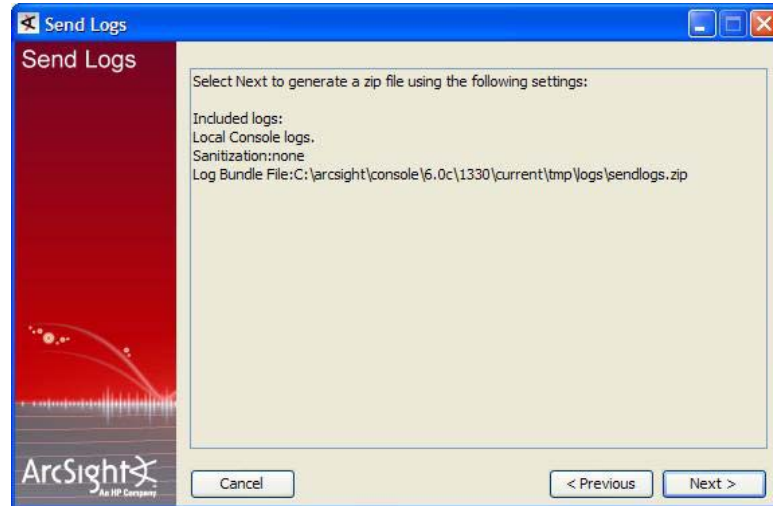


The 'Send Logs' dialog box has a blue title bar and a red sidebar with the ArcSight logo. The main area is white and contains the following text: 'Enter the incident number that HP Software Support Online gave you.' and 'If you do not have an incident number, please contact HP Software Support Online before zipping logs.' Below this is a text input field labeled 'Incident Number'. At the bottom are four buttons: 'Cancel', '< Previous', and 'Next >'.

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

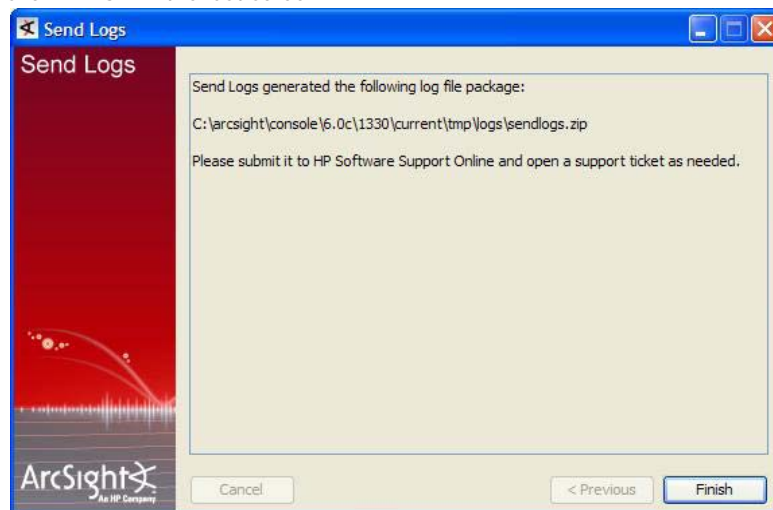
In case you do not have an incident number at this time, you can continue by entering a meaningful name for the compressed file to be created. Once you obtain the incident number from Customer Support, you can rename the file with the incident number you received.

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



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

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



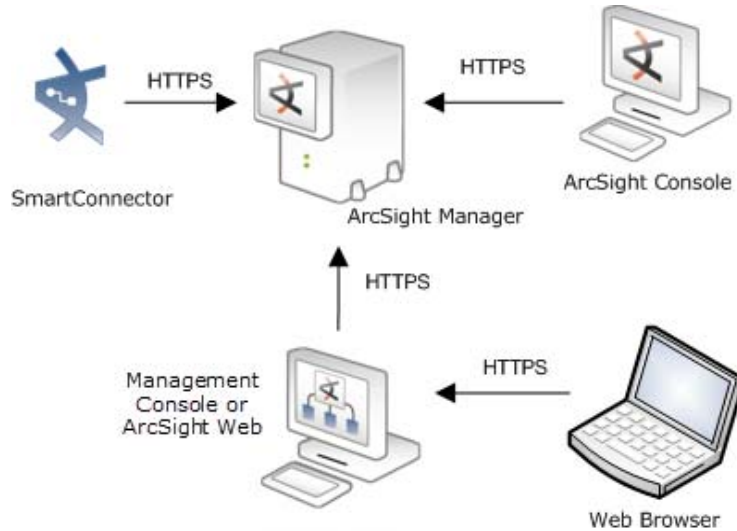
Understanding SSL Authentication

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

SSL enables the Manager (referred to as a “server”) to authenticate to its clients and communicate information over an encrypted channel, thus providing the following benefits:

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

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



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

Terminology

These terms are used in describing and configuring SSL:

- Certificate

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

- Key pair

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



Note

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

The `keytoolgui` utility is discussed in ["Tools for SSL Configuration" on page 38](#).

- SSL server-SSL client

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

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

- Keystore

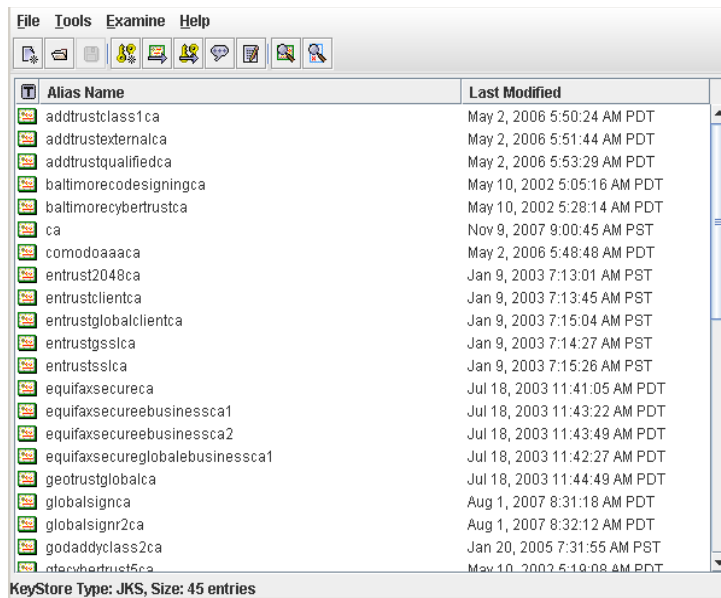
A keystore is an encrypted repository on the SSL server that holds the SSL certificate and the server's private key. The following table lists the ESM component, the name of the keystore on that component, and its location.

Log File	keystore File Name[2]	Location of keystore
Manager	keystore	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webkeystore	<ARCSIGHT_HOME>/config/jetty
Clients[1] (for client-side authentication)	keystore.client	<ARCSIGHT_HOME>/config

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

[2] 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 of the issuers that a client trusts.



The `keytoolgui` utility, used to view a truststore, is discussed in [“Tools for SSL Configuration” on page 38](#).

Note

When an issuer issues a certificate to the server, it signs the certificate with its private key. When the server presents this certificate to the client, the client uses the issuer's public key from the certificate in its 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 44](#).

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

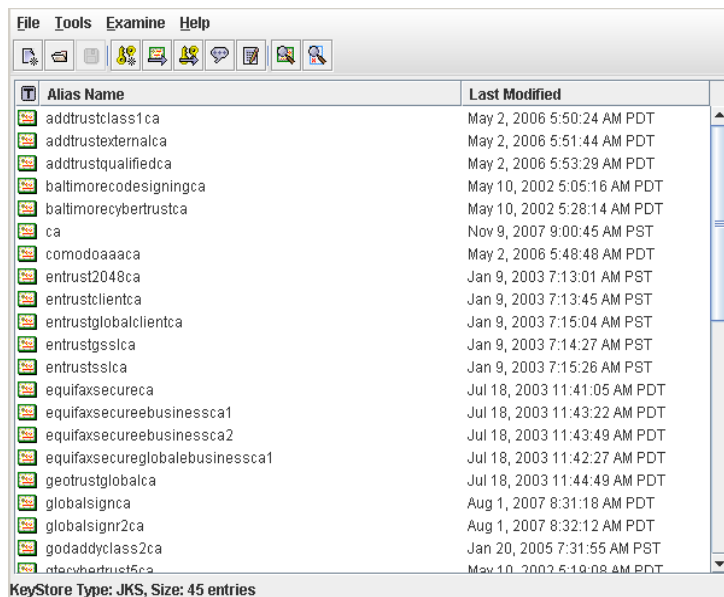
Component	truststore File Name	Location of truststore
Clients	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	cacerts[1]	<ARCSIGHT_HOME>/jre/lib/security
ArcSight Web	cacerts	<ARCSIGHT_HOME>/jre/lib/security
Manager	truststore[2]	<ARCSIGHT_HOME>/config/jetty
ArcSight Web	webtruststore[2][3]	<ARCSIGHT_HOME>/config/jetty

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

[2] When client-side authentication is used.

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

■ Alias



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

■ Truststore password

The `*.defaults.properties` file contains the default truststore password for each ESM component (*changeit*). The password is in clear text and typically, you do not need to change it. To change or obfuscate it, use the `changepassword` utility, as described in [Appendix A, Administrative Commands](#), on page 115. The following table lists the property name where the obfuscated truststore passwords are stored.

Truststore	Property File	Property Name
Client	client.properties**	ssl.truststore.password

Truststore	Property File	Property Name
Manager*	server.properties	servletcontainer.jetty311.truststore.password.encrypted
ArcSight Web	webserver.properties	servletcontainer.jetty311.truststore.password.encrypted
Connector	agent.properties**	ssl.truststore.password

*For client-side authentication

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

■ Keystore password

Use a keystore password to encrypt the keystore file and use a truststore password to encrypt a truststore file. Without this password, you cannot open these files.

The default is *password* for the Manager and ArcSight Web, and *changeit* for the ArcSight Console's client keystore. The default password for the key pair for any component is the same as for the component's keystore.

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

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

*For client-side authentication

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

■ NSS database password

The default password for the Manager's nssdb, the Console's nssdb.client, and ArcSight Web's webnssdb are all *changeit*. To change it, see ["Changing the Password for NSS DB" on page 213](#).

■ Cacerts password

The default password for cacerts is *changeit*.

■ Cipher suite

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

The following cipher suites are enabled by default:

- ◆ TLS_RSA_WITH_AES_128_CBC_SHA

- ◆ SSL_RSA_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_RSA_WITH_RC4_128_MD5
- ◆ SSL_RSA_WITH_RC4_128_SHA

Other supported cipher suites are:

- ◆ TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- ◆ TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- ◆ SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_RSA_WITH_DES_CBC_SHA
- ◆ SSL_DHE_RSA_WITH_DES_CBC_SHA
- ◆ SSL_DHE_DSS_WITH_DES_CBC_SHA
- ◆ SSL_RSA_EXPORT_WITH_RC4_40_MD5
- ◆ SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- ◆ SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- ◆ SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- ◆ SSL_RSA_WITH_NULL_MD5
- ◆ SSL_RSA_WITH_NULL_SHA
- ◆ SSL_DH_anon_WITH_RC4_128_MD5
- ◆ TLS_DH_anon_WITH_AES_128_CBC_SHA
- ◆ SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- ◆ SSL_DH_anon_WITH_DES_CBC_SHA
- ◆ SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- ◆ SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

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

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

Cipher suites are set as a comma-delimited list in the `ssl.cipher.suites` property. During the SSL handshake, the client provides this list as the cipher suites that it can accept, in descending order of preference. The server compares the list with its own set of acceptable cipher suites, picks one to use based on its order of preference, and communicates it to the client.

Tools for SSL Configuration

Keytoolgui

The `keytoolgui` utility enables you to perform a number of SSL configuration tasks on Windows. Some of these tasks are:

- [“Using Keytoolgui to Export a Key Pair” on page 39](#)
- [“Using Keytoolgui to Import a Key Pair” on page 39](#)

- [“Using Keytoolgui to Export a Certificate” on page 40](#)
- [“Using Keytoolgui to Import a Certificate” on page 41](#)
- [“Creating a keystore Using Keytoolgui” on page 42](#)
- [“Generating a Key Pair Using Keytoolgui” on page 43](#)

■

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

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

```
./arcsight keytoolgui
```

On SmartConnectors, use:

```
./arcsight agent keytoolgui
```

Using Keytoolgui to Export a Key Pair

- 1 To start it, run 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 37](#).
- 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 37](#).
- 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**.

Using Keytoolgui to Import a Key Pair

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

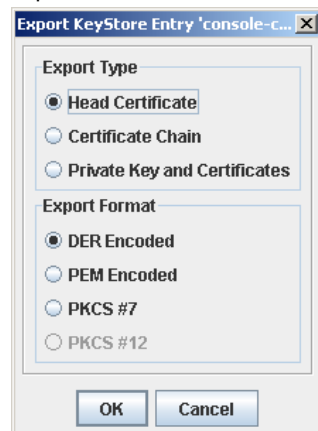
```
./arcsight keytoolgui
```
- 2 Select **File->Open keystore** and navigate to your component's keystore.
- 3 Enter the keystore password when prompted. For the default password see [“Keystore password” on page 37](#).
- 4 Select **Tools->Import Key Pair** and navigate to the location of the key pair 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 37](#).
- 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.

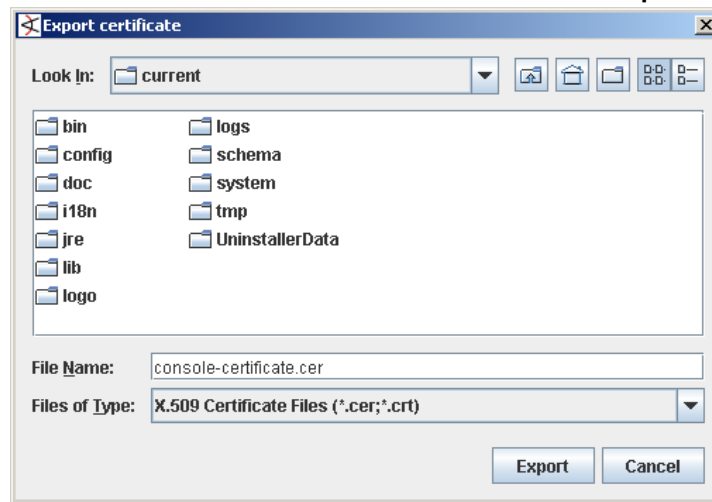
Using Keytoolgui to Export a Certificate

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

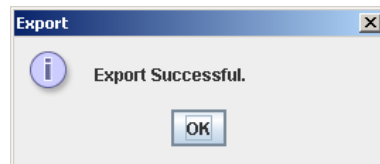
```
./arcsight keytoolgui
```
- 2 Select **File->Open keystore** and navigate to your component's truststore.
- 3 Enter the truststore password when prompted. For the default password see [“Truststore password” on page 36](#).
- 4 Right-click the certificate and select **Export**.
 - e Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- f** 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**.



- g** You see the following message:



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

Using Keytoolgui to Import a Certificate

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

```
./arcsight keytoolgui
```
- 2** Click **File->Open keystore** and navigate to the truststore (`<ARCSIGHT_HOME>/jre/lib/security`) of the component.
- 3** Select the store named `cacerts` and click **Open**.
- 4** Enter the password for the truststore when prompted. For the default password see ["Truststore password" on page 36](#).
- 5** Click **Tools->Import Trusted Certificate** and navigate to the location of the certificate that you want to import.
- 6** Click **Import**.

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



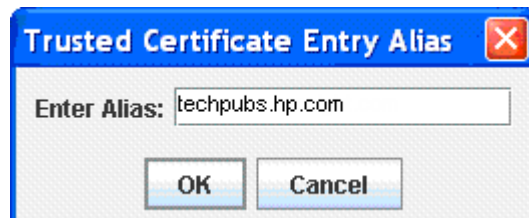
- 8 The Certificate details are displayed. Click **OK**.

- 9 You see the following message. Click **Yes**.



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

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



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



- 12 Save the truststore file.

Creating a keystore Using Keytoolgui

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

```
./arcsight keytoolgui
```

- 2 Click **File->New keystore**.

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

Generating a Key Pair Using Keytoolgui

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

```
./arcsight keytoolgui
```

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

Viewing Certificate Details

- 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 36](#).
- 4 Double-click the certificate whose details you want to view. Details include valid date range, and other information about the certificate.

keytool

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

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

To use `keytool`, enter this command:

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

where <store value> can be:

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

On SmartConnector hosts, use:

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

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

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

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

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

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

tempca

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

```
./arcsight tempca
```

On SmartConnectors, use:

```
./arcsight agent tempca
```

Two frequently performed operations using this utility are:

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

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

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

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.

SSL certificates

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

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

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

Types

You can use three types of SSL certificates:

- CA-signed

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

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

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

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

Comparing Self-signed and CA-signed certificates

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

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

Viewing Certificate Information

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

For the `nssdb`, `nssdb.client`, and `webnssdb`, use the `runcertutil` command to view certificate information. See ["runcertutil" on page 150](#), for more information.

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

Using a Demo Certificate

You can only use a demo certificate in default mode. It is only available when setting up the Manager. It is not recommended for production environments. To use a demo certificate:

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

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

```
runagentsetup
```

- b** In the SmartConnector Configuration Wizard, select **Yes, the ArcSight Manager is using a demo certificate**.

3 On a Console:

- a** Run this command in <ARCSIGHT_HOME>/bin:

```
consolesetup
```

- b** In the Console Configuration Wizard, select **Yes, the ArcSight Manager is using a demo certificate**.

4 On ArcSight Web server:

- a** Run this command in <ARCSIGHT_HOME>/bin/opt/arcsight/web/bin:

```
webserversetup
```

- b** In the Web Configuration Wizard, select **Demo key pair** in the screen that prompts you to select the certificate type.

5 On web browsers connecting to ArcSight Web, you do not need to set anything; however, the browsers display a security dialog every time they connect. To stop a browser from displaying this dialog:

- a** In <ARCSIGHT_HOME>/bin/opt/arcsight/web/bin, run this command on the Manager machine to export the demo CA's certificate:

```
arcsight tempca -dc
```

A file named `demo.crt` is created in your current working directory.

- b** Import the `demo.crt` file into your web browser.

See your Web browser's documentation for details.

Using a Self-Signed Certificate

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

When clients communicate with one Manager

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

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

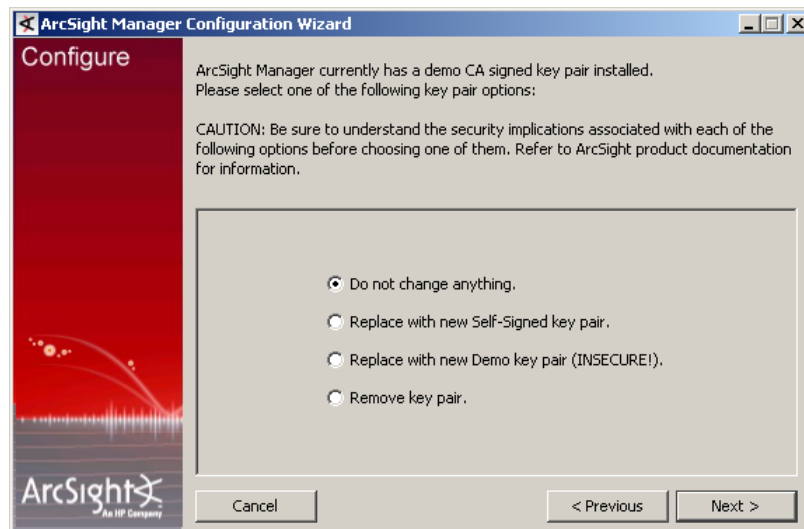


Steps to create a self-signed key pair may be different for a new Manager installation as the Configuration Wizard is launched automatically during the installation process.

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

```
./arcsight managersetup
```

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

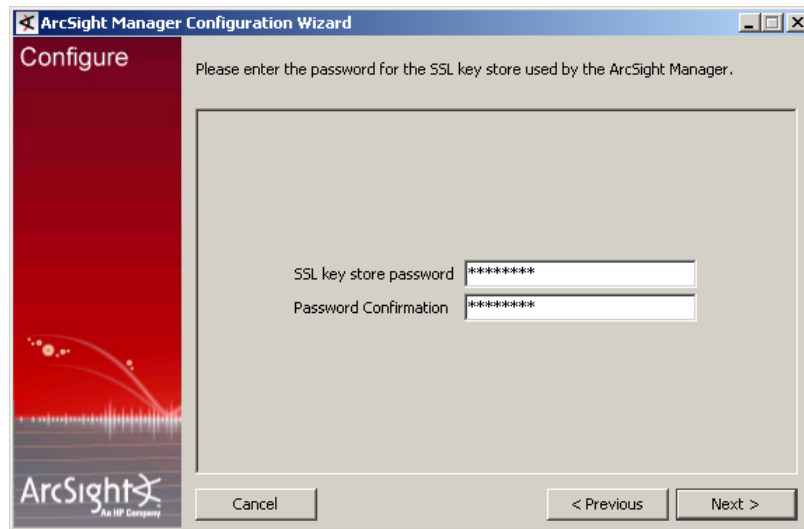


- c Enter information about the SSL certificate, as shown in this example. Click **Next**.



- d Enter the SSL keystore password for the certificate. Click **Next**.

Remember this password. You use it to open the keystore.



- e Step through the Configuration Wizard.

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

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



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

Note



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

Note

- 2 Export the Manager's certificate from `<ARCSIGHT_HOME>/jre/lib/security/cacerts`.
- 3 Make sure to copy the Manager's certificate to each machine from which clients connect to the Manager.
- 4 Import the Manager's certificate to the `<ARCSIGHT_HOME>/jre/lib/security` directory on all clients. See ["Using Keytoolgui to Import a Certificate" on page 41](#).



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.

Note

- 5 Restart the Manager process so that the Manager can start using the self-signed certificate.

- 6 Restart all clients.
- 7 When installing a new client, repeat Steps 2-4 of this procedure.
- 8 On the ArcSight Web server, perform the steps listed in section [“Setting up SSL Client Authentication on ArcSight Web”](#) on page 65.
- 9 On the ArcSight Console, perform the steps listed in section [“Setting up SSL Client-Side Authentication on ArcSight Console”](#) on page 58.

When clients communicate with multiple Managers

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



Note

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

- 1 Follow Step 1 from the previous procedure on all Managers.
- 2 Copy the selfsigned.cer file from all Managers to the `<ARCSIGHT_HOME>/jre/lib/security` directory on one of your clients.

To prevent a certificate file from overwriting another when you copy multiple certificate files with the same name to the same location, rename each certificate file as you copy. For example, copy the certificate file from ManagerA and rename it to `SelfSigned_MgrA.cer`.
- 3 On that client, use the `keytoolgui` utility to import certificates into the truststore (cacerts):
 - a In `<ARCSIGHT_HOME>/bin`, run this command:

`./arcsight keytoolgui`
 - b Click **File->Open keystore**.
 - c In `<ARCSIGHT_HOME>/jre/lib/security`, select the store named cacerts. For the default password see [“Cacerts password”](#) on page 37.
 - d Click **Tools->Import Trusted Certificate**:
 - i Select the self-signed certificate for a Manager and click **Import**.
 - ii You see the following message. Click **OK**.

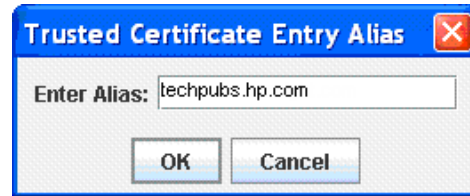


The Certificate details are displayed. Click **OK**.

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



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



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



- vi Save the truststore file.
- vii Repeat Steps i through vi for all self-signed certificates you copied.
- e On the client, enter this command in `<ARCSIGHT_HOME>/bin` to stop the client from using the currently in-use Demo certificate:

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

For SmartConnectors, run:

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

- 4 Repeat this cacerts procedure on all other clients.
- 5 Restart the Manager service so that the Manager can start using the self-signed certificate.
- 6 Restart the client.
- 7 When installing a new client, copy the cacerts file from any client you updated earlier in this procedure.

Using a CA-Signed SSL Certificate

Using certificate signed by a Certificate Authority means replacing your demo or self-signed certificate. You should obtain two CA-signed certificates—one for the Manager and the other for ArcSight Web, unless both components are installed on the same machine. Follow the procedure described in this section to obtain and import the certificates to the Manager, and if appropriate, to ArcSight Web.

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

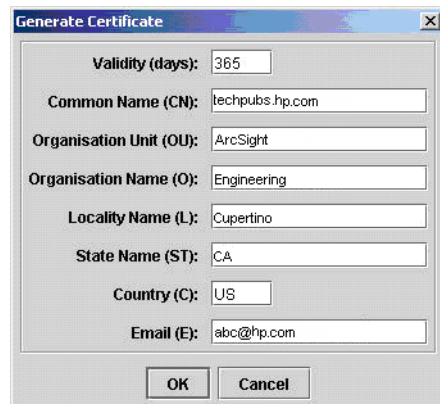
- 1 Create a Key Pair for a CA-Signed Certificate.
- 2 Send for the CA-Signed Certificate.
- 3 Import the CA Root Certificate.
- 4 Import the CA-Signed Certificate.
- 5 Restart the Manager.
- 6 Accommodating Additional Components.

Create a Key Pair for a CA-Signed Certificate

To Create a key pair:

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


```
./arcsight keytoolgui
```
- 2 Click **File->New keystore** to create a new keystore.
- 3 Select **JKS** for the keystore Type, it supports Java keystore:
- 4 Click **Tools->Generate Key Pair** to create the key pair. This can take some time.
- 5 Enter key pair information such as the length of time for its validity (in days). Click **OK**.



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

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

When you click **OK** it asks you for a new password. Use the password of your existing keystore to save this keystore. Also, 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 password, run the Manager setup Wizard and change the password of your existing keystore before you proceed. You reuse this file after receiving the reply from the CA.

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

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

Send for the CA-Signed Certificate

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

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

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

Import the CA Root Certificate

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

- 1 Save the Root CA certificate as a file `rootca.cer`.
- 2 Repeat the following procedure on all the machines where the Manager is installed:
 - a Launch the `keytoolgui` utility on the Manager machine.
 - b Click **File > Open keystore**.
 - c Select the Truststore file located at `<ARCSIGHT_HOME>/jre/lib/security/cacerts`. Use the default password to open `cacerts`. For the default password see ["Cacerts password" on page 37](#).
 - d Click **Tools > Import Trusted Certificate**, and pick the `rootca.cer` file.
 - e You see the following warning message:
"Could not establish a trust path for the certificate. The certificate information will now be displayed after which you may confirm whether or not you trust the certificate."
 - f Click **OK** to finish.



Note

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

Import the CA-Signed Certificate

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

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

```
-----BEGIN CERTIFICATE-----
MIICjTCCAfagAwIBAgIDWnWvMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQT
EiMCAGA1UECBMZrk9SIFRFU1RJTkcGUUVFSUE9TRVMgT05MWTEdMBsGA1UEChMUVGhh
d3RlIENlcnRpZmljYXRpb24xZzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQ
QDExNUaGF3dGUgVGZzdCBDQSBsb290MB4XDTAyMDkyNzIzMzI0MVoXDTAyMTAxODIz
MzI0MVowaDELMAkGA1UEBhMCrVMxDTALBgNVBAGTBGJsYWgxDTALBgNVBACTBGJsYW
gxDTALBgNVBAoTBGJsYWgxDTALBgNVBAsTBGJsYWgxHTAbBgNVBAMTFHppZXIuc3Yu
YXJjc2lnaHQy29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b
+BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vwN4JViC

CSBkDpiqVF7K11Sx4ZVSXX4+VQ6k4gT5G0kDNvQeN05wWkzEMygmB+ZBnYqPA/XtWR
ZtjxvH

MoqS+JEqHruimLITC6q0reUB/txby6+S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHS
UEDDAKBggrBgEFBQcDATAMBgNVHRMBAg8EAjAAMA0GCSqGSIb3DQEBAUAA4GBAFY3
7E60+P4b3zTLnaG7EVM57GtkeD6PwCIilB6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQV
QxnpABjzTalRfYgjNfJ6ltI6ZKjBO5kim9UBeCnKiNNzhIyDyFwbHXOPB/JaLIV+jG
ugYNS7hf/ay0BXKlfueO07EgjhB/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 Using any text editor, copy and paste the text string to a file. Include the line "-----BEGIN CERTIFICATE-----" and line "-----END CERTIFICATE-----", and make sure there are no extra spaces before or after the string.
- 3 Save it to a file named `ca_reply.txt` on the Manager in the `<ARCSIGHT_HOME>/config/jetty` directory.
- 4 On the Manager machine, run this command in `<ARCSIGHT_HOME>/bin`:

`./arcsight keytoolgui`
- 5 Click **File->Open keystore** and select the keystore (**keystore.request** or **webkeystore.request**) you saved in [Step 7](#) in "Create a Key Pair for a CA-Signed Certificate" on page 52. 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*.
- 7 Select **Import CA Reply** from the menu.
- 8 Select the CA reply certificate file and click **Import**.

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

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

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

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

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

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

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

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

- 12 For successful reconfiguration and Manager startup, enter the keystore passwords into the appropriate properties file.

Enter the password into the `webserver.properties` file for ArcSight Web using the following command (all on one line):

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

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

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

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

- 13 If your Manager clients trust the CA that signed your server certificate, go to ["Restart the Manager" on page 56](#).

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

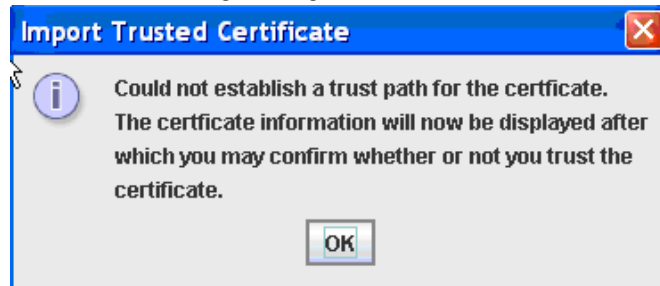


Also perform these steps on the Manager to update the Manager's cacerts so that Manager clients such as the archive utility can work.

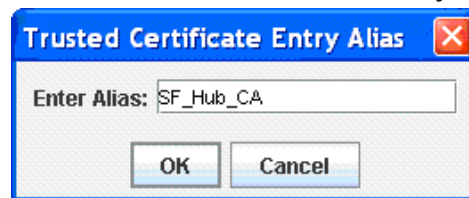
- a Obtain a root certificate from the CA that signed your server certificate and copy it to your client machine.
- b For one client, use the `keytoolgui` utility to import the certificate into the truststore (cacerts):
 - i In `<ARCSIGHT_HOME>/bin`, run this command:

```
./arcsight keytoolgui
```
 - ii Click **File->Open keystore**.

- iii Select the store named cacerts. Use the default password to open cacerts. For the default password see [“Cacerts password” on page 37](#).
- iv Click **Tools->Import Trusted Certificate** and select the certificate you copied in Step 10a of this procedure.
- v You see the following message. Click **OK**.



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



- vii Right-click the alias **ca** in the truststore and choose **Delete** from the menu.
 - viii Save the keystore.
- c** Copy the <ARCSIGHT_HOME>/jre/lib/security/cacerts file from the client in the previous step to all other clients.
- 14** If your ArcSight Web browser clients trust the CA that signed your ArcSight Web certificate, go to [Restart the Manager](#).

Otherwise, perform these steps:

- a** Obtain a root certificate from the CA that signed your ArcSight Web certificate.
- b** Import the certificate into your web browser. See your browser's documentation for details.

Restart the Manager

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

- 1** Restart the Manager.

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

- 2** Restart all clients.

- 3** To verify that the new certificate is in use:

- a** From the command line navigate to <ARCSIGHT_HOME> and enter the command: `arcsight tempca -i`

The output shows which CA issuer signed the SSL CA-signed certificate, certificate type, status of a validation of the certificate, and so on.

- b** Point a web browser to `https://<manager_hostname>:8443`. to test it.

Accommodating Additional Components

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

- **Adding additional Managers**

You do not need to add the CA root certificate to the Truststore-cacerts file again. However, you must copy the cacerts file from the existing Manager to the new Manager.

- **Other ArcSight Components (Console, ArcSight Web, and SmartConnectors).**

When installing a new Console, you must copy the 'cacerts' file from the existing Console, which has been updated in the Phase 3, to the newly installed Console. This configuration procedure of Manager Ca-signed SSL certificate can be applied on the ArcSight Web server unless both components are installed on the same machine.

For ArcSight Web, use the `webserversetup` utility after the certificate is updated to confirm the certificate is valid, as follows:

- a** Login as an ESM user on the ArcSight Web server machine.
- b** Execute the following command from `<ARCSIGHT_HOME>/bin`:


```
./arcsight webserversetup
```
- c** Restart the ArcSight Web server.

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

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

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

- 2** Replace the certificate by importing the new certificate into truststore/cacerts as the case may be. Use the `keytoolgui` to import the new certificate into the truststore or cacerts. See [“Using a Demo Certificate” on page 46](#), [“Using a Self-Signed Certificate” on page 47](#), or [“Using a CA-Signed SSL Certificate” on page 51](#) section (depending on the type of certificate you are importing) for steps on how to import the certificate.

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

Establishing SSL Client Authentication

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

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



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

Setting up SSL Client-Side Authentication on ArcSight Console

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

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

```
./arcsight keytoolgui
```

- b Open **File->New keystore**. This opens the New keystore Type dialog.

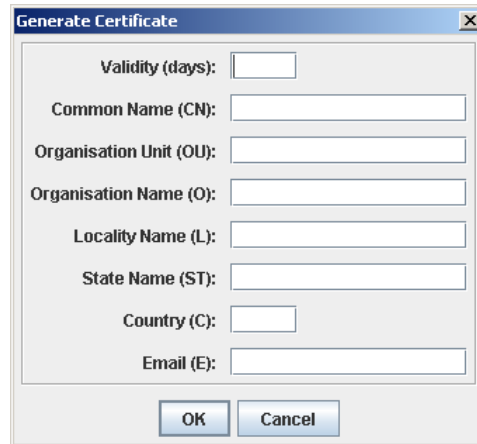
- c Select **JKS** and click **OK**.



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



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

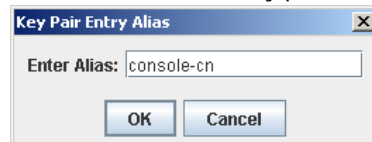


Generate Certificate dialog box with the following fields:

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

Buttons: OK, Cancel

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



Key Pair Entry Alias dialog box with the following field:

- Enter Alias:

Buttons: OK, Cancel



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

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

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

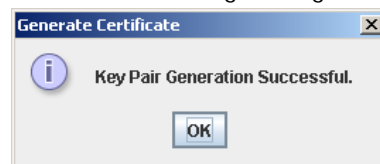


Key Pair Entry Password dialog box with the following fields:

- Enter New Password:
- Confirm New Password:

Buttons: OK, Cancel

- g You see the following message.

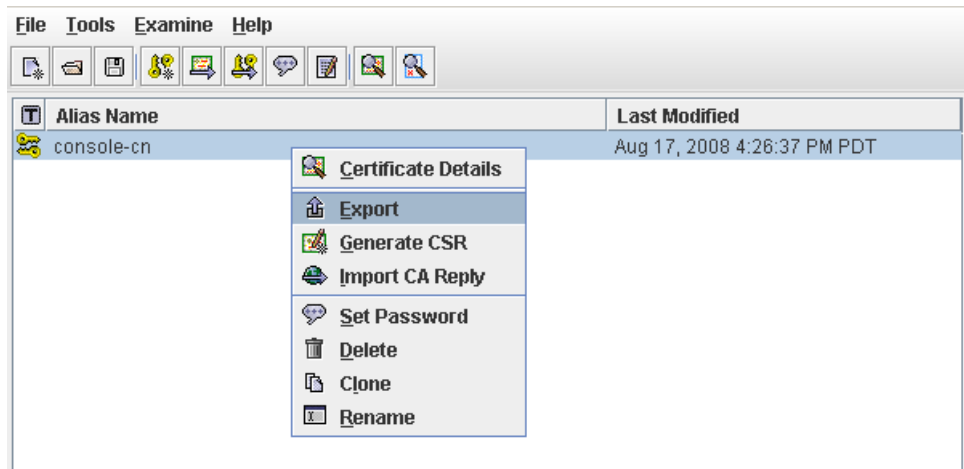


Generate Certificate dialog box showing the message: Key Pair Generation Successful.

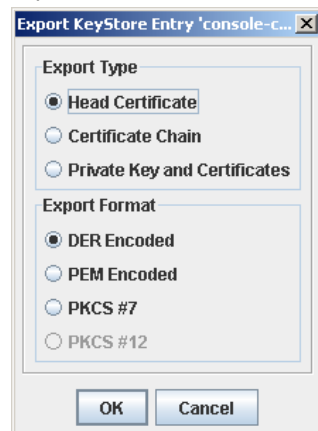
Button: OK

- 2 Export the key pair you just generated.

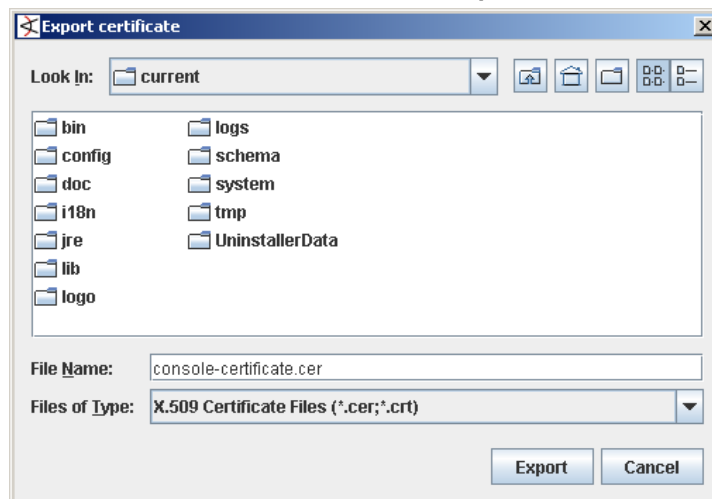
- a** In the keytoolgui right-click the key pair you just generated and select **Export**.



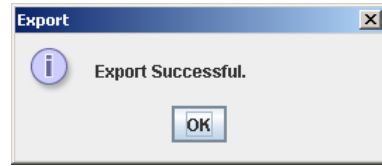
- b** Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



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



- d You see the following message:



- e If your Console is on a different machine than the Manager, copy this certificate to the Manager's machine.

- 3 If you are using self-signed certificate skip this step and continue with step 4.

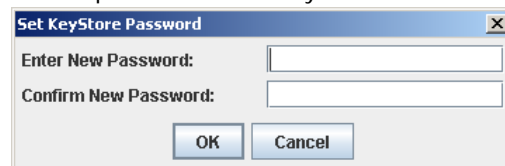
Import the signed certificate response in the keystore of all Consoles.

- ◆ Import the signed certificate response in the Console's keystore, `keystore.client`. Follow the steps in section ["Import the CA Root Certificate" on page 53](#).
- ◆ Use the `changepassword` tool to set an encrypted keystore password in the `client.properties` file:

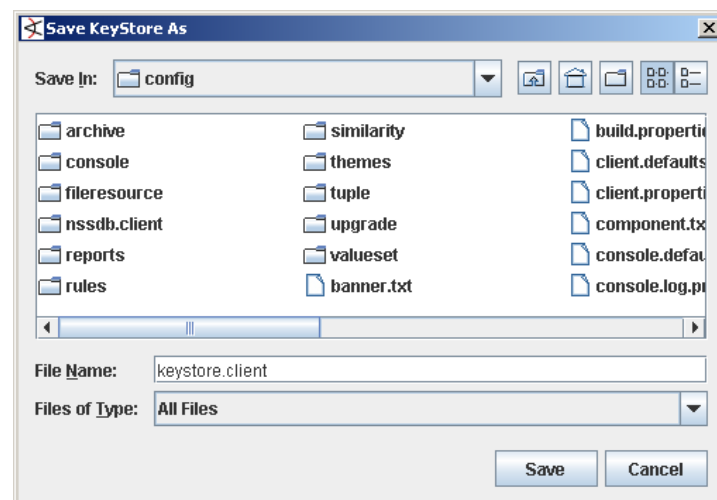
```
arcsight changepassword -f config/client.properties -p
ssl.keystore.password
```

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

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



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



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

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

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

```
ssl.client.auth=true
```

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

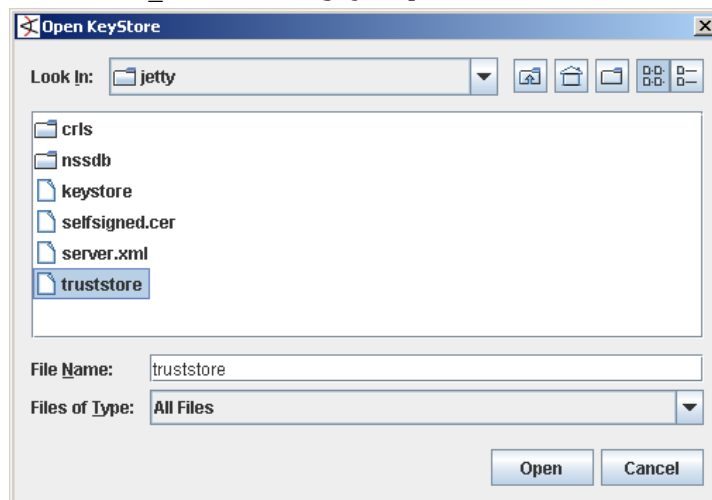
- 6 Use the `changepassword` tool to set an encrypted keystore password in the `client.properties` file:

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

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

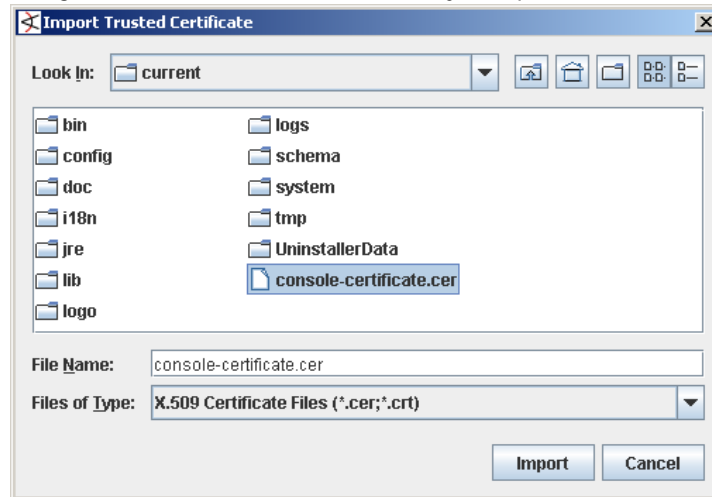
If your Manager trusts the CA that signed your Console's certificates, go to the next step. Otherwise perform these steps to update the Manager's truststore.

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



- c Enter *password* when prompted for the password and click **OK**.
- d Click **Tools->Import Trusted Certificate**.

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



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



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

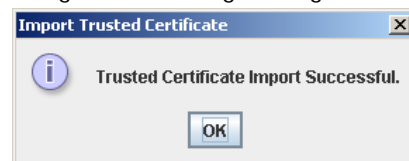
- h Click **Yes** in the following dialog.



- i Enter an alias for the certificate.



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

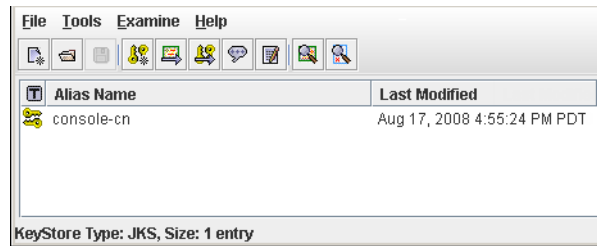


- k Click **OK** and save the changes to the truststore.

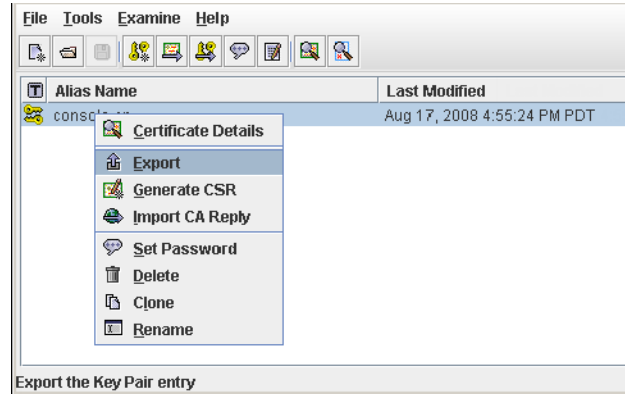
- 8 Export the Console's private key. If you use ArcSight Web, you are required to import the Console's private key into the Web browser you use with ArcSight Web.

- a Start the keytoolgui from the Console's `bin` directory.

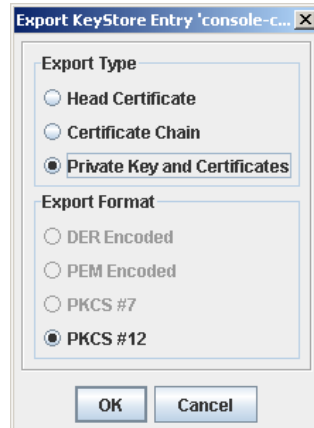
- b Click on **File->Open keystore** and navigate to the Console keystore you created.



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

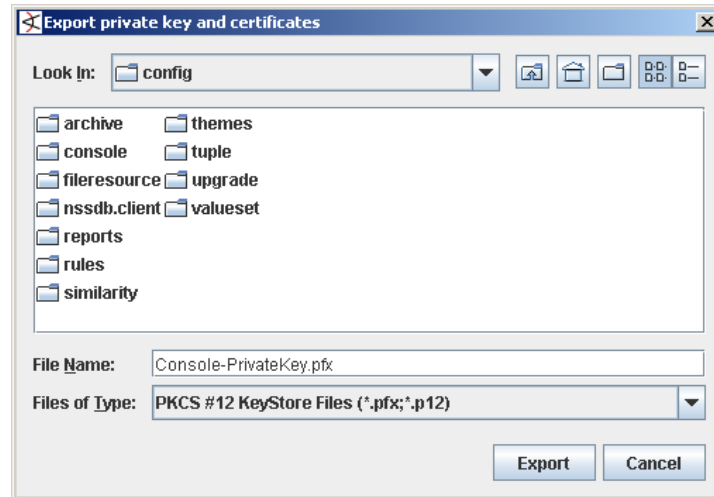


- d Select **Private Key and Certificates** as Export Type and **PKCS#12** as the Export Format if not already selected and click **OK**.

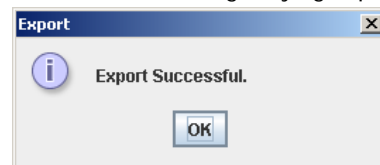


- e Enter the password that you had set for the Console's keystore when prompted and click **OK**.
- f Enter a new password for the keystore and confirm the password and click **OK**.

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



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



- 9** Exit keytoolgui.
- 10** Restart the Manager.
- 11** Restart ArcSight Console.

Setting up SSL Client Authentication on ArcSight Web

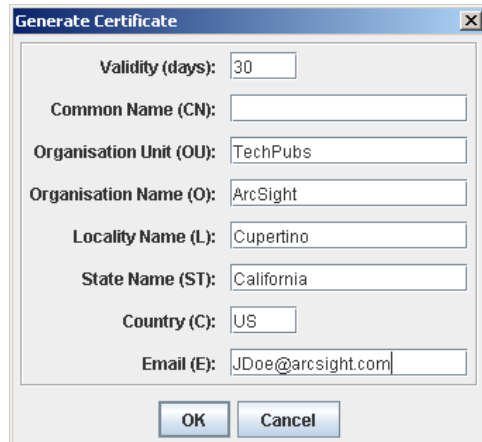
To enable client-side authentication for clients running in default mode, perform these steps in addition to the ones you perform for setting up server authentication:

- 1** Generate a key pair on ArcSight Web. For CA-signed certificate follow the steps in section ["Create a Key Pair for a CA-Signed Certificate" on page 52](#)
 - a** From the Web's <ARCSIGHT_HOME>/bin directory start the keytoolgui by running the following command:


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



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



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

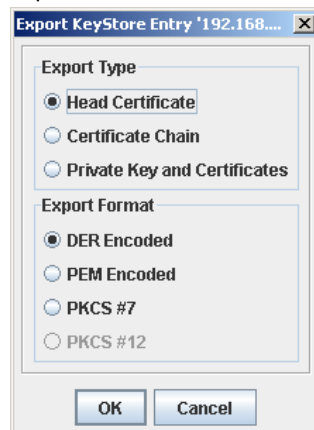
Field	Value
Validity (days):	30
Common Name (CN):	
Organisation Unit (OU):	TechPubs
Organisation Name (O):	ArcSight
Locality Name (L):	Cupertino
State Name (ST):	California
Country (C):	US
Email (E):	JDoe@arcsight.com

Buttons: OK, Cancel

**Note**

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

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

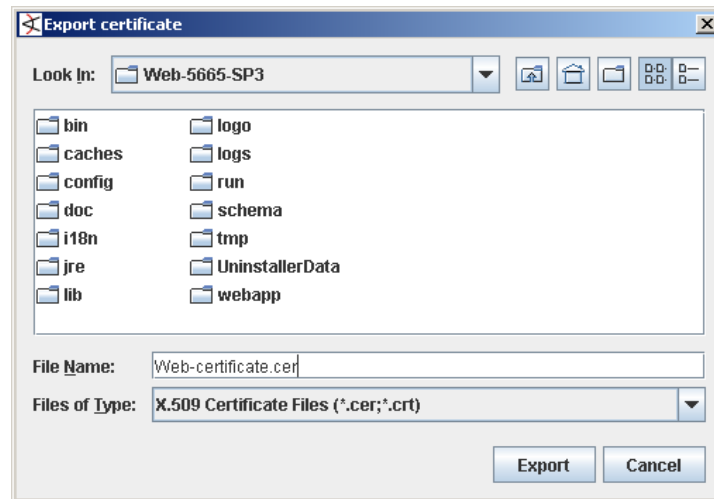


The 'Export KeyStore Entry' dialog box shows the following settings:

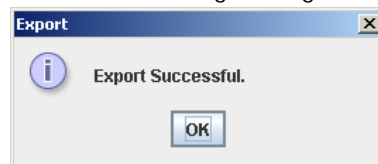
Section	Selected Option
Export Type	Head Certificate
Export Format	DER Encoded

Buttons: OK, Cancel

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

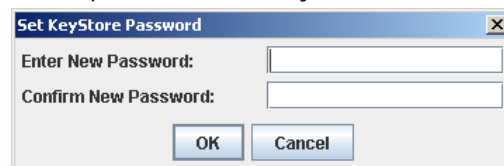


- d You see the following message:



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

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



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

- 4 If you are using self-signed certificate skip this step and continue with step 5.

Import the signed certificate response in the keystore of ArcSight Web.

- ◆ Import the signed certificate response in the Web's keystore. Follow the steps in section ["Import the CA Root Certificate" on page 53](#).
- ◆ Use the changepassword tool to set an encrypted keystore password in the client.properties file:

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

- 5 Add the following properties in the Web's <ARCSIGHT_HOME>/config/client.properties file and save the file:

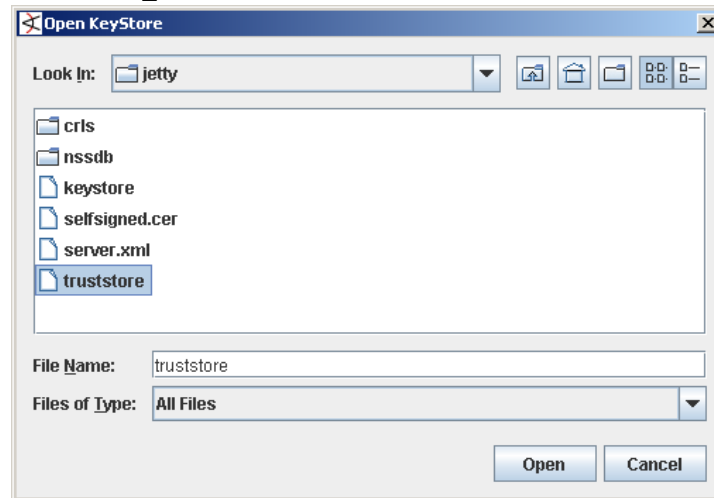
```
ssl.keystore.password=<password-set-when-you-saved-the-
keystore>
```

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

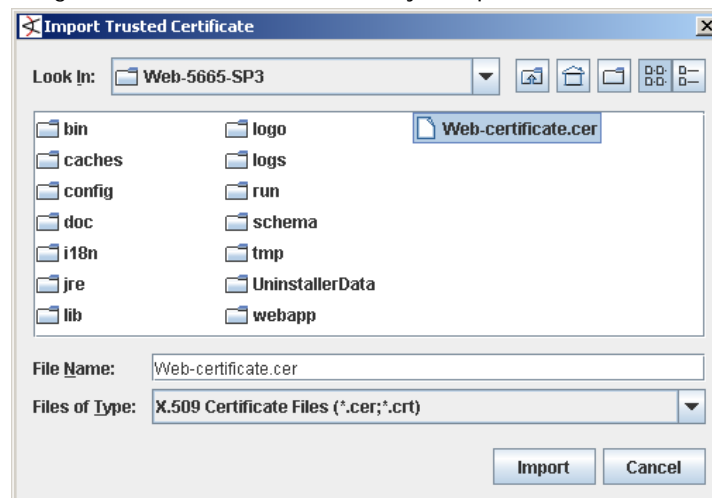
- 6 Import Web's key pair into the Manager's truststore.

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

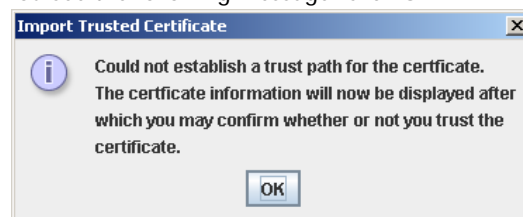
- a Start the keytoolgui by entering `arcsight keytoolgui` command from the Manager's bin directory.
- b Click **File->Open keystore** and navigate to `<ARCSIGHT_HOME>/config/jetty/truststore`.



- c Enter the password when prompted and click **OK**. For the default password see ["Keystore password" on page 37](#).
- d Click **Tools->Import Trusted Certificate**.
- e Navigate to the Web's certificate that you exported earlier and click **Import**.

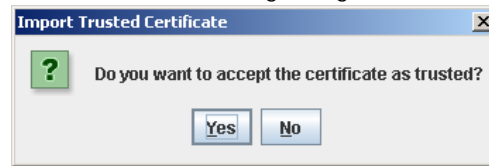


- f You see the following message. Click **OK**.



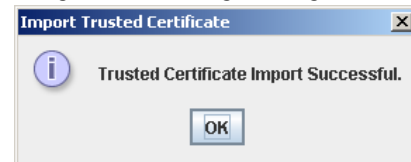
g Review the certificate details and click **OK**.

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



i Enter an alias for the certificate.

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



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

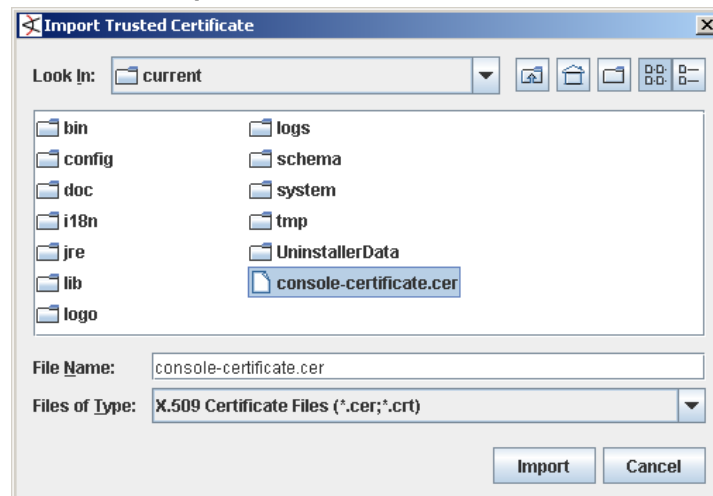
7 Import Console's certificate into webtruststore.

a Start the keytoolgui from ArcSight Web's bin directory.

b Click **File->Open keystore** and navigate to the Web's
<ARCSIGHT_HOME>/config/jetty/webtruststore.

c Enter the password when prompted. For the default password see ["Keystore password" on page 37](#).

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



e Navigate to the Console's certificate and click **Import**.

f Click **OK** in the next message box prompting you that "Could not establish a trust path for the certificate..."

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

h Click **Yes** when prompted whether you want to accept the certificate as trusted.

i Enter an alias for the console's certificate and click **OK**.

j You see a message saying "Trusted Certificate Import Successful."

- k** Click **OK**.
- l** Save changes to the webtruststore and exit the keytoolgui.
- 8** Import the following into the web browser that you use with ArcSight Web:
 - ◆ Web's certificate you exported in [Step 2 on page 66](#) above.
 - ◆ Console's private key you created in [Step 8 on page 63](#) in section "Setting up SSL Client-Side Authentication on ArcSight Console" on page 58.

See your web browser's documentation for steps to do the above.
- 9** Restart the Manager.
- 10** Restart ArcSight Web.

Setting up Client-side Authentication on Partition Archiver and SmartConnectors

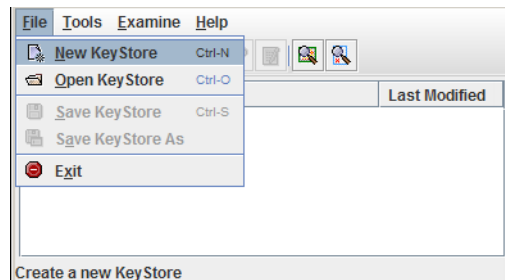
In order to enable client-side authentication on clients (Partition Archiver and/or SmartConnectors) running in default mode, perform these steps:

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

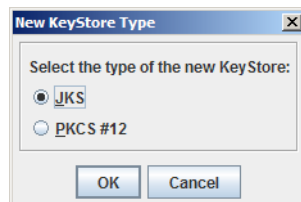
```
./arcsight agent keytoolgui
```

 On Partition Archiver:

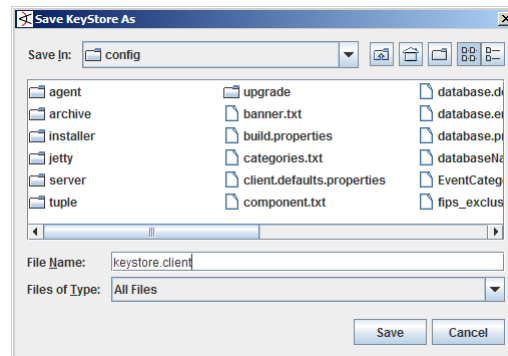
```
arcsight keytoolgui
```
 - b** Go to **File->New keystore**.



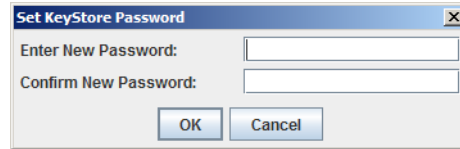
- c** Select **JKS** for type of keystore and click **OK**.



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

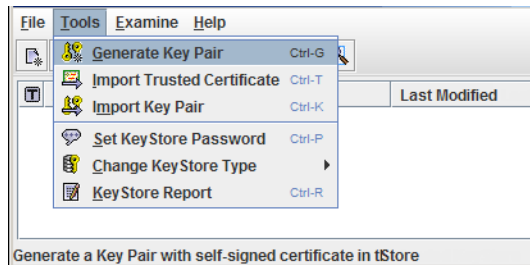


- e Set a password for the keystore and click **OK**.

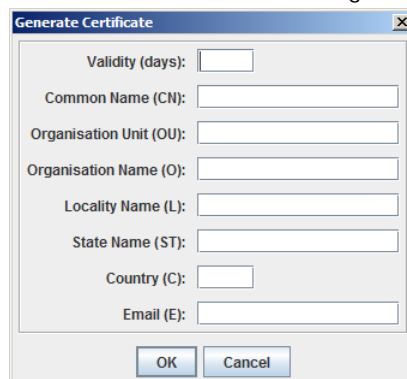


- 2 Create a new key pair in the `config/keystore.client` of the ArcSight Database or SmartConnector. (If you already have a keypair that you would like to use, you can import the existing key pair into the client's `config/keystore.client`. See section [“Using Keytoolgui to Import a Key Pair” on page 39](#) for details.)

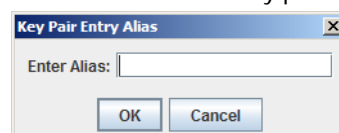
- a In keytoolgui, click **Tools->Generate Key Pair**.



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



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



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



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

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

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



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

- 4 Export the client's (Partition Archiver or Connector) certificate using `keytoolgui`. See section ["Using Keytoolgui to Export a Certificate" on page 40](#) for details.
- 5 Import the CA's certificate of the client's certificate (in case you are using CA-signed certificate) or the client's certificate itself (in case you are using a self-signed certificate) into the Manager's truststore, `/config/jetty/truststore`. see section ["Using Keytoolgui to Import a Certificate" on page 41](#) for details.
- 6 Restart the Manager.
- 7 Restart the client (Partition Archiver or Connector).

Migrating from one certificate type to another

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

Migrating from Demo to Self-Signed

To migrate from a demo to self-signed certificate:

- 1 Follow the steps described in ["Using a Self-Signed Certificate" on page 47](#).
- 2 Follow the instructions in ["Verifying SSL Certificate Use" on page 73](#) to ensure that a self-signed certificate is in use.

Migrating from Demo to CA-Signed

To migrate from a demo to CA-Signed certificate:

- 1 Follow the steps described in ["Using a CA-Signed SSL Certificate" on page 51](#).
- 2 Follow the instructions in ["Verifying SSL Certificate Use" on page 73](#) to ensure that CA-signed certificate is in use.

Migrating from Self-Signed to CA-Signed

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

- 1 Follow the steps described in [“Using a CA-Signed SSL Certificate” on page 51](#).
- 2 Follow the instructions in [“Verifying SSL Certificate Use” on page 73](#) to ensure that a CA-signed certificate is in use.

Verifying SSL Certificate Use

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

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

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

- 1 Review the value of the line: Demo CA trusted.
The value should be “no.”
If the value is “yes,” the demo certificate is still in use. Follow these steps to stop using the demo certificate:
 - a In <ARCSIGHT_HOME>/bin, enter the following command to make the client stop using the currently in use demo certificate:


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

 For SmartConnectors, run:


```
./arcsight agent tempca -rc
```
 - b Restart the client.
- 2 Verify that the Certificate Authority that signed your certificate is listed in the output. For a self-signed certificate, the Trusted CA 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 on the Windows platform:

```
ArcSight TempCA starting...

SSL Client
truststore C:\arcsight\Console\current\jre\lib\security\cacerts
  Type                JKS
  Demo CA trusted     no
  Trusted CA          DigiCert Assured ID Root CA
[digicertassuredidrootca]
  Trusted CA          TC TrustCenter Class 2 CA II
[trustcenterclass2caii] .
.
Demo CA
  keystore    C:\arcsight\Console\current\config\keystore.tempca
Exiting...
```

Using Certificates to Authenticate Users to ArcSight

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

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



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

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

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

Using the Certificate Revocation List (CRL)

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

Before you use the CRL feature, make sure:

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

To use the CRL feature:

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

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

Reconfiguring the ArcSight Console after Installation

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

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

```
./arcsight consolesetup
```

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

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

The ArcSight Console Configuration Wizard appears.

Reconfiguring ArcSight Manager

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

```
./arcsight managersetup
```

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

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

The Manager Configuration Wizard appears to help you re-configure the Manager. The `managersetup` wizard is covered in [“Running the Manager Configuration Wizard” on page 95](#).

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

Changing ArcSight Manager Ports

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

The Manager uses a single port (by default, 8443) that any firewalls between the Manager, ArcSight Console, and any ArcSight SmartConnectors must allow communication through. Port 8443 is the default port used when initially installing ArcSight, however, you can

change this default port number using the Manager Configuration Wizard. For more information, refer to the ESM Installation and Configuration Guide.

Changing ArcSight Web Session Timeouts

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

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

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

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

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

```
<session-config>

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

</session-config>
```

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

Managing Password Configuration

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

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

Requiring Mix of Characters in Passwords

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

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

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

```
auth.password.letters.min=-1
auth.password.letters.max=-1
auth.password.numbers.min=-1
auth.password.numbers.max=-1
auth.password.whitespace.min=0
auth.password.whitespace.max=0
auth.password.others.min=-1
auth.password.others.max=-1
```

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

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

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

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

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

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

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

Checking Passwords with Regular Expressions

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

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

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

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



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

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

■ `auth.password.regex.match= /^\D.*\D$/`

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

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

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

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

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

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

- ◆ At least two upper case letters
- ◆ At least two lower case letters
- ◆ At least two digits

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

Password Uniqueness

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

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

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



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

Note

Setting Password Expiration

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

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

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

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

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

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

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

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

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

Restricting the Number of Failed Log Ins

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

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

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

Once a user account has been disabled, the Manager can be configured to automatically re-enable it after a certain period of time. This reduces administrative overhead, while

effectively preventing brute force attacks. This mechanism is controlled by the following key in `server.properties`:

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

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

Disabling Inactive User Accounts

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

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

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

Re-Enabling User Accounts

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

Inspect/Editor panel in the ArcSight Console.

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

```
./arcsight reenableuser username
```

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

Properties Related to Domain Field Sets

Domain field sets are a construct in the Oracle ArcSight Database schema that make it possible to distinguish between events that pertain to different business verticals, such as credit card transactions, online banking, or stock transactions. Domain fields are not available for the CORR-Engine.

The domain field sets feature is separately licensed, and requires some additional configuration on both the Manager and relevant SmartConnectors. See [Chapter 14, Domain Field Sets, on page 463](#) in the ArcSight Console User's Guide for details on this feature.

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

- `domain.event.relevance.percentage`

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

For example, if you set this property to

`domain.event.relevance.percentage=0.8`, and the additional data in the event has five fields, if four out of these five fields match the fields defined for a domain, the event is considered to have an 80% match. Since you set this property to .8 (or 80%), the event becomes tied to that domain and those four fields are persisted. The fifth field, which does not match, is dropped. If all five fields match, all of them are persisted. On the other hand, if only three fields match, the percentage is less than the 80% minimum you specified, so the event is not tied to the domain and all fields (even those that match) are dropped.

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

- `domain.ad.keywords.csv`

You can specify which Additional Data field names to exclude when processing additional data in an event. You can specify the field names to exclude by setting them in this property. Separate field names with a comma. For example, to exclude integer and date, set `domain.ad.keywords.csv=Integer,Date`.

- `turbo.enabled=false`

Turbo mode works by eliminating certain fields to speed throughput. That includes domain fields. Turbo mode is enabled by default during installation, even if you have licensed the Domains feature, so be sure to turn it off.

- `domain.off=false`

This property might already be set to `false` by default in the `server.defaults.properties` file when you have a Domains license. If you have to change it, do so in the `server.properties` file.

Restart the Manager after changing any of these properties.

If both turbo mode and Domains are turned on, the `server.std.log` file continuously produces “fatal exception” messages with instructions to turn off one or the other.

Advanced Configuration for Asset Auto-Creation

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

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

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

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

Asset Auto-Creation from Scanners in Dynamic Zones

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

Create Asset with either IP Address or Host Name

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

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

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



Caution

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

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

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

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

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

Preserve Previous Assets

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

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



Caution

Preserving previous assets results in a larger asset model.

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

When the system is configured with `scanner-event.dynamiczone.asset.nonidentifiable.create=false` and `scanner-event.dynamiczone.asset.ipconflict.preserve=true`, it takes the following actions:

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

Changing the Default Naming Scheme

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

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

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

```
myhost_1.1.1.1
```

In this case, change the default

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

to

```
$!destinationHostName_$destinationAddress
```

Compression and Turbo Modes

Compressing SmartConnector Events

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

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

```
compression.enabled = false
```

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

Reducing Event Fields with Turbo Modes

If your configuration, reporting, and analytic usage permits, you can accelerate the transfer of sensor information through SmartConnectors by choosing one of the "turbo" modes, which send fewer event fields from the connector. The default transfer mode is called Complete, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).

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

ESM defines the following Turbo Modes:

Turbo Modes		
1	Fastest	Recommended for firewalls
2	Faster	Manager default

When Turbo Mode is not specified (mode 3, Complete), all event data arriving at the SmartConnector, including additional data, is maintained. (Versions of ArcSight prior to 3.2 ran in Turbo Mode 3.) Turbo Mode 2, Faster, eliminates the additional custom or vendor-specific data, which is not required in many situations. Turbo Mode 1, Fastest, eliminates all but a core set of event attributes, in order to achieve the best throughput. Because the event data is smaller, it requires less storage space and provides the best performance. It is ideal for simpler devices such as firewalls.

The 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.

Turbo Mode and Domain Fields

Turbo mode excludes domain fields. If you purchased a license for domain fields, and wish to use them, you cannot also use turbo mode. To disable turbo mode and use the Domains feature:

- 1 Set `turbo.enabled=false` in the Manager `server.properties` file.
- 2 Set `domain.off=false`.
- 3 Restart the Manager.

Turbo mode is enabled by default during installation, even if you have licensed the Domains feature. If you want to use turbo mode and not the Domains feature:

- 1 Set `domain.off=true` and in the Manager `server.properties` file. Leave `turbo.enabled=true`.
- 2 Restart the Manager.

If both turbo mode and Domains are turned on, the `server.std.log` file continuously produces “fatal exception” messages with instructions to turn off one or the other.

Configuring the ArcSight Database Monitor

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

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

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

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

For more information about database checks performed to monitor configuration and runtime attributes of your database, see [Appendix C, Monitoring Database Attributes, on page 177](#).

Configuring Database Monitor e-mail message recipients

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

Configuring the check for free space in Oracle tablespaces

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

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

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

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

Sending Events as SNMP Traps

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

Configuration of the SNMP trap sender

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



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 compliant.

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

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

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

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

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

The system uses the filter specified by the URI (it should all be on one line) to decide whether or not an event is forwarded. There is no need to change the URI to another filter. These contents are locked and are overwritten when the contents are upgraded to the next version. By default, the "SNMP Trap Sender" filter logic is Matches Filter (Correlated Events)—that is, only rules-generated events are forwarded.

```
snmp.destination.host=
```

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

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

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

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

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

```
snmp.version=1

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

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

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

The SNMP field types are converted as:

ArcSight	SNMP
STRING	OCTET STRING
INTEGER	INTEGER32
Address	IP ADDRESS
LONG	OCTET STRING
BYTE	INTEGER

Additional data values are accessible by name, for example:


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

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

Asset Aging

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

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
```



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

Note

Task to Disable Assets of a Certain Age

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

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

To Delete an Asset

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

```
# Delete assets when they age

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

Amortize Model confidence with scanned asset age

The `IsScannedForOpenPorts` and `IsScannedForVulnerabilities` 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 and "old" asset gets no points. You can edit the `AmortizeScan` value (number of days) in the Manager's `/config/server/ThreatLevelFormula.xml` file:

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

For this example, the value is modified as follows:

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

Configuring Actors

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

- 1 Install the Actor Model Import connector appropriate for your IDM.** For complete instructions about how to install the connector, see the relevant SmartConnector installation and configuration guide, such as the SmartConnector Configuration Guide for Microsoft Active Directory Actor Model. Once installed, the connector polls the IDM and imports the user data into the Actor model.

- 2 Identify the authenticators in your environment.** In preparation for configuring the authenticator mapping table, open the dashboard for automatically identifying the user authentication data stores running in your environment and their type:

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

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

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



- 3 Configure the Authenticators mapping table.** Using the information gathered in step 2, fill out the account authenticators mapping table provided at /All Active Lists/ArcSight System/Actor Data Support/Account Authenticators. The data you enter here must exactly match the values displayed in the Actor Administration dashboard.

- a** In the Navigator panel, go to **Lists > Active Lists**. Right-click the active list /All Active Lists/ArcSight System/Actor Data Support/Account Authenticators and select **Show Entries**.
- b** In the Account Authenticator Details tab in the Viewer screen, click the add icon (+).
- c** For each account authenticator data store, enter the following data:

Column	Description
Device Vendor	The vendor that supplies the authentication data store, such as Microsoft.
Device Product	Provide the application name of the authentication system, such as Active Directory.
Agent Address	The IP address of the reporting SmartConnector.
Agent Zone Resource	The zone in which the reporting SmartConnector resides.

Column	Description
Authenticator	Enter the exact value(s) returned for Authenticator in the Actor Administration dashboard from the previous step, including punctuation, capitalization, and spaces. Using the example shown in the previous step, the value you would enter in this column would be: Active Directory: arcsight.com

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

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

Tuning Guide for Supporting Large Actor Models

If your actor model contains tens of thousands of members, follow the guidelines in this section to allow adequate processing capacity for best results.

- 1 Shut down the Manager
- 2 **Increase settings in `server.properties`.** Increase the following default values to support managing large blocks of actors by setting following properties in the `config/server.properties` file:

Server Property Name	Default Setting [units]	Comments
<code>dbconmanager.provider.oracle.pool.maxcheckout</code>		
	600 [seconds]	The maximum time for a database connection before the process is terminated. This setting comes into play when you want to delete a large block of actors from the ArcSight Console. The default value should be increased by a factor of 3-6x, for example, 1800 to 3600.

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

For instructions about how to run the `managersetup` utility, see the *Administrator's Guide*.

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

For details about starting and stopping the Manager, see “Basic Administration Tasks” in the *Administrator's Guide*.

For details about working with the `server.properties` file, see “Managing and Changing Properties File Settings” in the *Administrator's Guide*.

Permissions Required to Use Actor-Related Data

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

To create actors, actor channels, and category models:

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

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

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

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

Read access on the following resources and groups:

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

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



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

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

For details about how to assign permissions to user groups, see [“Granting or Removing Resource Permissions” on page 626](#).

About Exporting Actors

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

For instructions about how to use the `export_system_tables` command-line utility, see the *Administrator's Guide*.

Chapter 3

Running the Manager Configuration Wizard

This chapter covers the following topics:

[“Running the Wizard” on page 95](#)
[“Authentication Details” on page 101](#)

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

Running the Wizard

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

```
/sbin/service arcsight_services stop manager
```

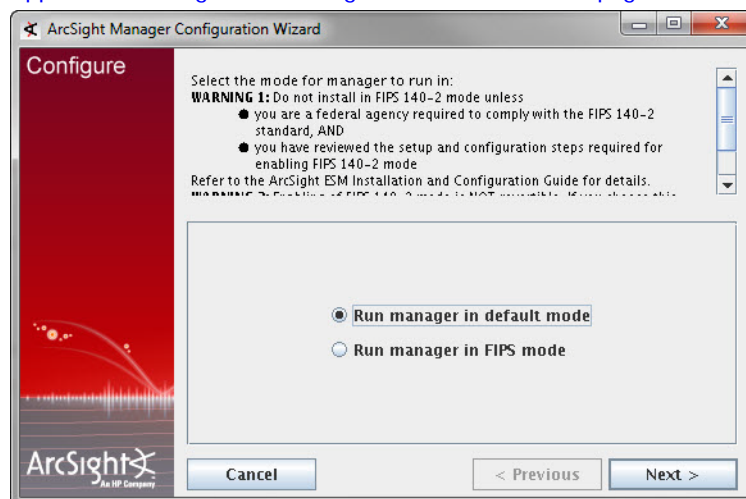
Verify that the Manager has stopped by running the following command (as user `arcsight`):

```
/sbin/service arcsight_services status all
```

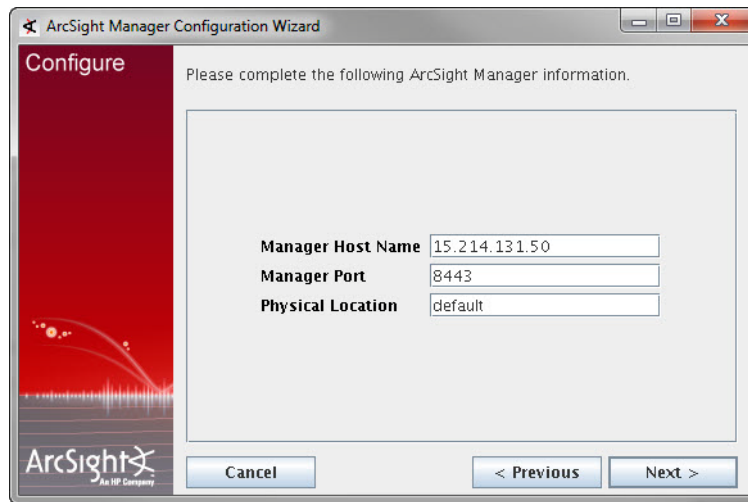
To start the wizard, run the following from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

- 1 Select whether you are using Default or FIPS mode. For information on FIPS, see [Appendix F, Configuration Changes Related to FIPS, on page 197](#)



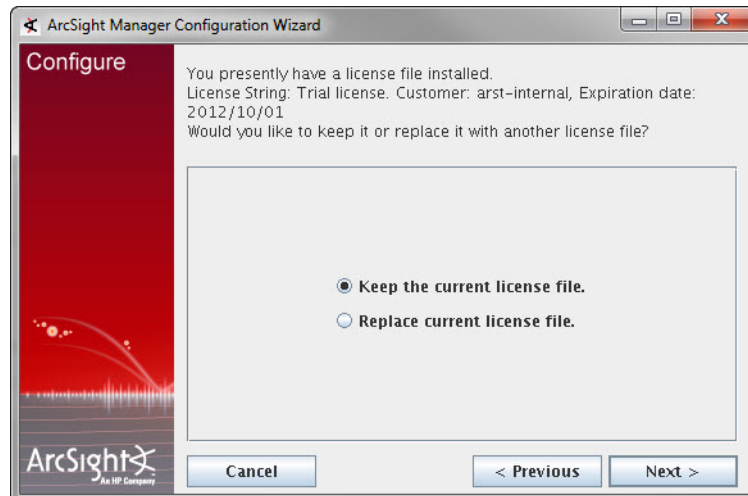
- 2 To change the hostname or IP address for your Manager host, enter the new one here. The Manager host name that you enter in this dialog appears on the Manager certificate. If you change the host name, be sure to regenerate the Manager's certificate in [Step 5 on page 97](#). We recommend that you do not change the Manager Port number.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. The main text says 'Please complete the following ArcSight Manager information.' Below this, there are three input fields: 'Manager Host Name' with the value '15.214.131.50', 'Manager Port' with the value '8443', and 'Physical Location' with the value 'default'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The ArcSight logo is visible in the bottom left corner.

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

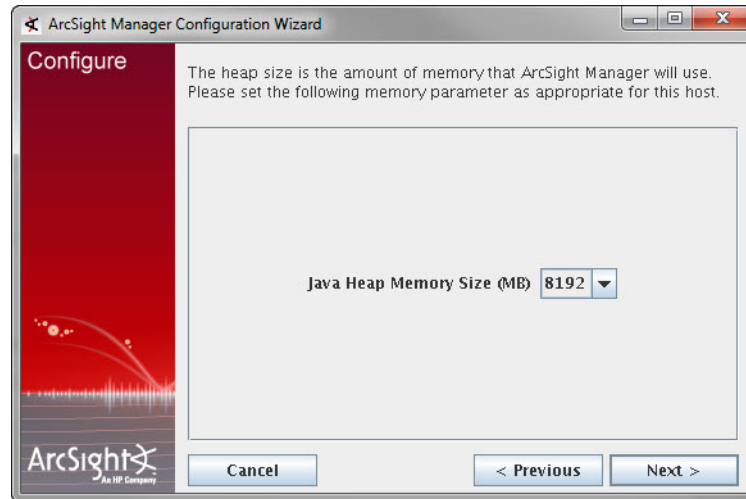
- 3 If you would like to replace your license file with a new one, select **Replace current license file**. otherwise accept the default option of **Keep the current license file**.



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

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

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



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

- 5 The Manager controls SSL certificate type for communications with the Console, so the wizard prompts you to select the type of SSL certificate that the Manager is using. If you changed the Manager host name in [Step 2 on page 96](#), 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 default in this screen and click **Next**.

ArcSight Manager Configuration Wizard

Configure

Please complete the following information about the database.

Logger JDBC URL

Database Password

Cancel < Previous Next >

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

ArcSight Manager Configuration Wizard

Configure

Please select a method for authenticating users with ArcSight Manager.

☒ Password Based Authentication

☐ Password Based and SSL Client Based Authentication

☐ Password Based or SSL Client Based Authentication

☐ SSL Client Only Authentication

Cancel < Previous Next >

- 8 Select the method for authenticating the users. See [“Authentication Details”](#) on page 101 for more details on each of these options.

ArcSight Manager Configuration Wizard

Configure

Please select a method for authenticating users with ArcSight Manager.

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

☒ Built-In Authentication

☐ RADIUS Authentication (SecurID, PremierAccess)

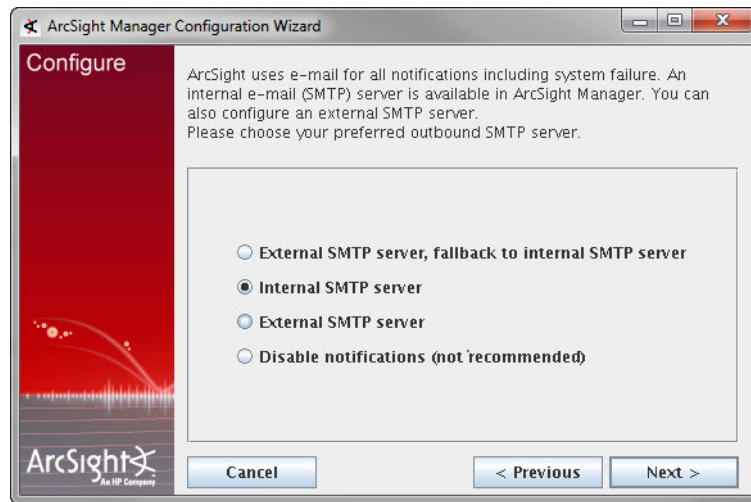
☐ Microsoft Active Directory

☐ Simple LDAP Bind

☐ Custom JAAS Plugin Configuration

Cancel < Previous Next >

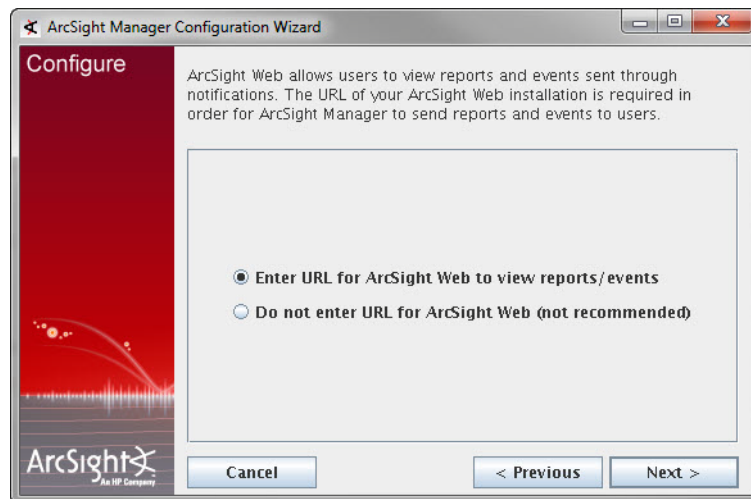
- 9 Accept the default and click **Next** or configure a different email server for notification.



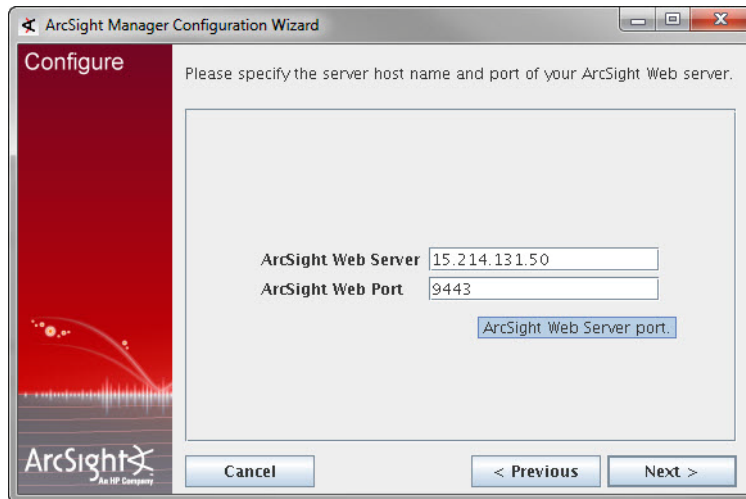
Caution

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

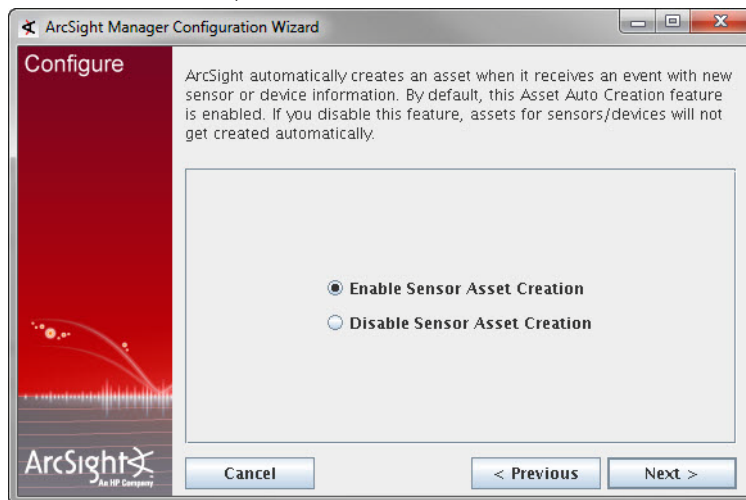
- 10 Select **Do not enter URL for ArcSight Web** and click **Next**.



- 11 Specify the ArcSight Web server and port.



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



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

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

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

```
/sbin/service arcsight_services start manager
```

Authentication Details

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



Caution

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

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

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

How external authentication works

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

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

Users who pass these checks are authenticated.

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

Guidelines for setting up external authentication

Follow these guidelines when setting up an external authentication mechanism:

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

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



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

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

Password Based Authentication

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

Built-In Authentication

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

If you selected this option, you are done.

Setting up RADIUS Authentication

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

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

Setting up Active Directory User Authentication

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

The next panel prompts you for this information.

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

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

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

Configuring AD SSL

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

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

Setting up LDAP Authentication

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

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

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

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



Note

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

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

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

Configuring LDAP SSL

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

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

Using a Custom Authentication Scheme

Choose the **Custom JAAS Plug-in Configuration** option if you want to use an authentication scheme that you have built. You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.

Password Based and SSL Client Based Authentication

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



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

Password Based or SSL Client Based Authentication

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

SSL Client Only Authentication

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

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

Chapter 4

Database Administration

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

[“Changing Oracle Initialization Parameters” on page 107](#)
[“Monitoring Available Free Space in Tablespaces” on page 108](#)
[“Setting Up Database Threshold Notification” on page 108](#)
[“Resetting the Oracle Password” on page 109](#)
[“Oracle Cold Backup” on page 109](#)
[“Oracle Hot Backup” on page 109](#)
[“Exporting Data” on page 110](#)
[“Recovering ArcSight Databases” on page 110](#)
[“Backing up ArcSight Databases” on page 109](#)
[“Partition logs” on page 111](#)



Caution

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

Changing Oracle Initialization Parameters

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

Changing these parameters is recommended only for experienced database administrators.

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

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

and, on Windows:

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

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

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

and, on Windows:

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

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

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

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

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

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

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

Monitoring Available Free Space in Tablespaces

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

Setting Up Database Threshold Notification

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

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

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

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

Resetting the Oracle Password

Depending upon your Oracle settings, you may need to reset your password from time to time. Oracle can be set to expire passwords, which lock out the Manager. To reset or renew the password for the ArcSight Database user (`arcsight` by default), log in to Oracle with `/ as sysdba` and run the following command:

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

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

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

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

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

```
arcsight managersetup
```

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

Backing up ArcSight Databases

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

Oracle Cold Backup

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

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

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

Oracle Hot Backup

Oracle Hot Backup is also an image backup of Oracle database files. But it only includes Oracle datafiles as part of its backup. This kind of backup is taken when the database is up and running. The database has to be operating in archive log mode before hot backup can be done. This backup when restored needs a database recovery applied to it from the online logs and archive logs after the database is mounted. Oracle tracks the changes

applied during the backup process by generating a lot of redo log files. An Oracle hot backup should be done every day on the primary or target system.

Exporting Data

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

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

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

Recovering ArcSight Databases

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

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

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

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

Speeding up partition compression

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

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

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

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

Partition logs

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

`partitionmanager.log`—For Partition Manager logs

`partitioncompressor.log`—For Partition Compressor logs

`partitionarchiver.log`—For Partition Archiver logs

`partitionstatisticsupdater.log`—For Partition Statistics Updater logs

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

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

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

Chapter 5

Managing Resources

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

This chapter in the ArcSight Console User's Guide....	...discusses these topics
Chapter 21, Managing Users and Permissions, on page 619	<ul style="list-style-type: none">• "Managing Users" on page 619• "Managing Permissions and Resources" on page 625• "Managing Notifications" on page 637
Chapter 24, Modeling the Network, on page 715	<ul style="list-style-type: none">• "Modeling the Network" on page 715• "Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories" on page 737• "Managing Customers" on page 750
Chapter 7, Filtering Events, on page 177	<ul style="list-style-type: none">• "Creating Filters" on page 177• "Moving or Copying Filters" on page 180• "Deleting Filters" on page 181• "Debugging Filters to Match Events" on page 181• "Applying Filters" on page 185• "Importing and Exporting filters" on page 186• "Using Filter Groups" on page 186• "Investigating Views" on page 187• "Modifying Views" on page 191

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

Chapter 22, Managing Resources, on page 645

- "Managing File Resources" on page 645
- "Locking and Unlocking Resources" on page 648
- "Selecting Resources" on page 649
- "Finding Resources" on page 650
- "Visualizing Resources" on page 653
- "Viewing Resources in Grids" on page 656
- "Validating Resources" on page 657
- "Extending Audit Event Logging" on page 662
- "Saving Copies of Read-Only Resources" on page 663
- "Common Resource Attribute Fields" on page 663
- "Managing Packages" on page 665

Chapter 23, Managing SmartConnectors, on page 677

- "Selecting and Setting SmartConnector Parameters" on page 677
- "Managing SmartConnector Filter Conditions" on page 694
- "Setting Special Severity Levels" on page 695
- "Sending Model Mappings to SmartConnectors" on page 697
- "Sending Control Commands to SmartConnectors" on page 697
- "Managing SmartConnector Groups" on page 704
- "Managing SmartConnector Resources" on page 705
- "Importing and Exporting SmartConnector Configurations" on page 706
- "Upgrading SmartConnectors" on page 708

Chapter 25, Managing Partitions, on page 753

- "Getting Partition Information" on page 753
 - "Seeing a Partition Schedule" on page 753
 - "Archiving Partitions" on page 754
 - "Reactivating Archived Partitions" on page 754
 - "Reactivating Zipped or Large Archived Partitions" on page 755
 - "Deactivating Archived Partitions" on page 755
 - "Running Scheduled Tasks Right Away" on page 756
 - "Partition Properties" on page 756
-

Appendix A

Administrative Commands

This appendix provides information about assorted Administrative commands.

[“ArcSight Commands” on page 115](#)

ArcSight Commands

Alphabetical ArcSight Commands List

ACLReportGen	dropSLPartitions	refcheck
agent logfu	exceptions	regex
agent tempca	export_system_tables	replayfilegen
agentcommand	flexagentwizard	resetpwd
agents	groupconflictingassets	resvalidate
agentsvc	idefensesetup	ruledesc
agenttempca	import_system_tables	runcertutil
agentup	keytool	runmodutil
arcdbutil	keytoolgui	runpk12util
arcdt	kickbleep	script
archive	listsubjectdns	searchindex
archivefilter	logfu	sendlogs
archivewizard	manager	tee
bleep	managerinventory	tempca
bleepsetup	manager-no-wrapper	testdbconnection
changepassword	manager-reload-config	threaddumps
checklist	managersetup	tproc
console	managerstop	uninstallservice
consolesetup	managersvc	webserver
database pc	managerthreaddump	webserver-no-wrapper
database pm	managerup	webserversetup
database xts	monitor	webserversvc
databasesetup	netio	websetup
dbcheck	package	whois
dbview-generator	portinfo	
deploylicense	querytuner	
downloadcertificate	reenableuser	

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

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

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

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

ACLReportGen

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

agent logfu

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

agent tempca

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

agentcommand

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

agents

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

agentsvc

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

agenttempca

Description	See the agent tempca command
Applies to	SmartConnectors

agentup

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

arcdbutil

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

Examples	<p>To identify all disabled rules in your current installation:</p> <pre>arcdbutil sql select name from arc_resource where id in (select id from arc_rules where active=0);</pre> <p>To get an SQL interface:</p> <pre>arcdbutil sql</pre> <p>Enter user-name: / as sysdba</p>
-----------------	--

arcdt

Description	A utility that enables you run diagnostic utilities such as database alert logs, session wait times, and thread dumps about your system, which helps Customer Support analyze performance issues on your components
Applies to	Manager
Syntax	arcdt diagnostic_utility utility_Parameters
Parameters	<div data-bbox="610 783 1360 926"> <p>diagnostic_utility Utilities you can run are:</p> <p>db-alertlog—Retrieve the database alert log from the database machine.</p> </div> <div data-bbox="610 947 1360 1346"> <p>db-alertlog—Retrieve the database alert log from the database machine. session-waits—Retrieve the currently running JDBC (Java Database Connection) sessions and their wait times.</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> </div> <div data-bbox="610 1367 1360 1822"> <p>-fmt <format> — The format the output should be displayed in (where relevant), choices are: html/text (text)</p> <p>-o <outputfile> — File name to save output to. ()</p> <p>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> </div>

	<pre> help help commands help <command> </pre>	Use these help Parameters (no dash) to see the Parameters, a list of commands, or help for a specific command.
Examples	<p>To retrieve the last 20 lines of database alert log from your database machine and save it to a file called 20110720_dblog, run this command:</p> <pre>arcsight arcdt db-alertlog -ln 20 -o 20110720_dblog</pre>	

archive

Description	<p>Import or export resources (users, rules, and so on) to or from one or more XML files.</p> <p>Note: Generally, there is no need to use this command. The Packages feature in the ArcSight Console is more robust and easier to use for managing resources.</p>	
Applies to	Manager, Console	
Syntax	archive -f <archivefile> [Parameters]	
Required Parameter	-f <archivefile>	<p>The input (import) or the output (export) file specification.</p> <p>Note: Filename paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME>, not the current directory.</p>
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>	<p>Configuration file to use.</p> <p>Default: config/server.defaults.properties</p>
	-conflict <conflictpolicy>	<p>The policy to use for conflicts resolution. Possible policies are:</p> <p>default: Prompts user to resolve import conflicts.</p> <p>force: Conflicts are resolved by the new overwriting the old.</p> <p>overwrite: Merges resources, but does not perform any union of relationships.</p> <p>preferpackage: if there is a conflict, it prefers the information in the package that is coming in over what is already there.</p> <p>skip: Do not import resources with conflicts.</p>

<code>-exportaction</code> <code><exportaction></code>	<p>The action to assign to each resource object exported. Export actions are:</p> <p>insert: Insert the new resource if it doesn't exist (this is the default).</p> <p>update: Update a resource if it exists.</p> <p>remove: Remove a resource if it exists.</p>
<code>-format <fmt></code>	<p>Specifies the format of the archive. If you specify nothing, the default is default.</p> <p>default: Prompts user to resolve import conflicts.</p> <p>preferarchive: if there is a conflict, it prefers the information that is coming in over what is there.</p> <p>install: Use this for the first time.</p> <p>update: Merges the archive with the existing content.</p> <p>overwrite: Overwrites any existing content.</p>
<code>-h</code>	Get help for this command.
<code>-i</code>	(Synonym for <code>-action import</code> .)
<code>-m <manager></code>	The Manager to communicate with.
<code>-newids</code>	All archival objects within an archive are given new IDs. All refs to these archival objects are changed to the new ID or removed if not found. This option is useful when an archive is created and then all resources in the archive are modified to create new resources but the IDs were retained.
<code>-o</code>	Overwrite any existing files.
<code>-p <password></code>	Password with which to log in to the Manager.
<code>-param</code> <code><archiveparamsfile></code>	The source file for parameters used for archiving. Any parameters in the named file can be overridden by command line values.
<code>-pc <configfile></code>	Private configuration file to override <code>-config</code> . Default: <code>config/server.properties</code>
<code>-pkcs11</code>	Use this option when authenticating with a PKCS#11 provider. For example, <code>arcsight archive -m <hostname> -pkcs11 -f <file path></code>
<code>-port <port></code>	The port to use for Manager communication. Default: 8443
<code>-q</code>	Quiet: do not output progress information while archiving
<code>-source <sourcefile></code>	The source file. This is used for all commands that use the <code>-f</code> to specify an output file and use a separate file as the input.

<code>-standalone</code>	<p>Operate directly on the Database, not the Manager.</p> <p>Warning: Do not run archive in <code>-standalone</code> mode when the Manager is running; database corruption could result.</p>
<code>-u <username></code>	<p>The user name to log in to the Manager</p>
<code>-uri <includeURIs></code>	<p>The URIs to export. No effect during import. All dependent resources are exported, as well—for example, all children of a group.</p> <p>Separate multiple URIs (such as <code>/All Filters/Geographic/West Coast</code>) with a space, or repeat the <code>-uri</code> switch</p>
<code>-urichildren</code> <code><includeURIchildren></code>	<p>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.</p>
<code>-xrefids</code>	<p>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.</p>
<code>-xtype <excludeTypes></code>	<p>The types to exclude during export. No effect during import. Exclude types must be valid type names, such as Group, Asset, or ActiveChannel.</p>
<code>-xtyperef</code> <code><excludeTypeRefs></code>	<p>The types to exclude during export (there is no effect during import). This is the same as <code>-xtype</code>, except it also excludes all references of the given type. These must include only valid type names such as Group, Asset, and ActiveChannel.</p>
<code>-xuri <excludeURIs></code>	<p>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.</p>
<code>-xurichildren</code> <code><excludeURIchildren></code>	<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

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

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

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

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

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

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

To export a specific resource:

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

Manual import (program prompts for password):

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

Scheduled or batch importing:

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

Scheduled or batch exporting:

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

Archive Command Details



Note

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

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

The `archive` command automatically creates the archive files you specify, saving resource objects in XML format. This documentation does not provide details on the structure of archive files and the XML schema used to store resource objects for re-import into the system. Generally it is easier to use packages.

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

Remote Mode

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

```
arcsight archive -u Username -m Manager [-p Password] -f Filename
```

```
[-i | -sort] [-q] ...
```

**Caution**

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

```
arcsight tempca -ac
```

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

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

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

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

Standalone Mode

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

**Caution**

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

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

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

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

**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 ["Understanding SSL Authentication" on page 33](#) 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. For example (on Windows):

```
arcsight archive -u admin -p password -m hostname
-f c:\archive\archive.xml
```

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



If the Manager is running, you must specify archive commands in remote mode, entering your user name, password, and Manager name to connect to the Manager. To run the archive command in standalone mode, accessing resources directly from the ArcSight Database, enter `-standalone` rather than `-u <username> -p <password> -m <manager>`.

- 3 Enter the number of the resource type to archive.

The `archive` command displays a list of options that let you choose which resource or group within the resource type that you want to archive.

- 4 Choose the resource or group to archive.

After making your selection, you are prompted whether you want to add more resources to the archive.

- 5 You can continue adding additional resources to the archive list. When you've finished, answer no to the prompt

Would you like to add more values to the archive? (Y/N)

After it is finished writing the archive file, you are returned to the command prompt.

Importing Resources from an Archive

- 1 Make sure the archive tool client can trust the Manager's SSL certificate. Refer to ["Understanding SSL Authentication" on page 33](#) for information on managing certificates.
- 2 From the <ARCSIGHT_HOME>/bin directory, type `arcsight archive` with its parameters and attach `-i` for import.



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 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"
```



You can specify multiple URI resources with the URI parameter keyword by separating each resource with a space character, or you can repeat the URI keyword with each resource entry.

archivefilter

Description	Use the command to change the contents of the archive. The archivefilter command takes a source archive xml file as input, applies the filter specified and writes the output to the target file.	
Applies to	Manager	
Syntax	archivefilter -source <sourcefile> -f <archivefile > [Parameters]	
Parameters	-a <action>	Action to perform {insert, remove, none} (Default: none)
	-e <element_list>	Elements to process (Default: '*' which denotes all elements)
	-extid <regex>	Regular expression to represent all of the external IDs to include. This is the external ID of the archival object. (Default: none)
	-f <file>	Target file (required). If a file with an identical name already exists in the location where you want to create your target file, the existing file is overwritten. If you would like to receive a prompt before this file gets overwritten, use the -o option

-o	Overwrite existing target file without prompting (Default: false)
-relateduri <regex>	Regular expression to get all of the URIs found in references to include. This checks all attribute lists that have references and if any of them have a URI that matches any of the expressions, that object is included
-source <file>	Source file (required)
-uri <regex>	Regular expression to represent all of the URIs to include. This is the URI of the archival object
-xe <element_list>	Elements to exclude
-xextid <regex>	Regular expression to represent all of the external IDs to exclude
-xgroups <groups>	Groups to exclude
-xuri <regex>	Regular expression to represent all of the URIs to exclude
-h	Help for this command

Examples

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

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

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

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

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

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

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

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

archivewizard

Description	Archive wizard
Applies to	Manager
Syntax	archivewizard
Parameters	None

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

bleep

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

bleepsetup

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

	-g	Generate sample properties file
Examples	To run: arcsight bleepsetup	

changepassword

Description	Command to change obfuscated passwords in properties files. The utility prompts for the new password at the command line	
Applies to	Manager	
Syntax	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	ArcSight Environment Check. Used internally by the installer to see if you have the correct JRE and supported OS and are connected to a supported Database. This can run from the Connector, Database, or Manager.
--------------------	---

console

Description	Run the ArcSight Console	
Applies to	Console	
Syntax	console [-i] [parameters]	
Parameters	-ast <file>	
	-debug	
	-i	
	-imageeditor	
	-laf <style>	Look and feel style: metal, plastic, plastic3d. The default style for Windows is different than these and not specified. For Unix it is Plastic3d.
	-p <password>	Password

	-port	Port to connect to Manager (default: 8443)
	-redirect	
	-relogin	
	-server	Manager host name
	-slideshow	
	-theme	
	-timezone <tz>	Timezone: such as "GMT" or "GMT-8:00"
	-trace	Log all Manager calls
	-u <name>	User name
Examples	To run the console:	
	ArcSight Console	

consolesetup

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

database pc

Description	Partition configuration command	
Applies to	Database	
Syntax	database pc	
Parameters	-d <db_type>	Database type: oracle, db2
	-i <mode>	Mode: silent

-f <file>	Properties filename. Required in -i silent mode
-g	Generate the SQL scripts
-s	Generate a sample properties file for use in -i silent mode
-x	Execute the existing SQL scripts
-p	Run this command in expert mode. If the statistics updates are timing out and the event rate is very high, then the sample size should be reduced to 0.1. Using the -p option with this command opens the wizard and allows you to change the sample size.
Examples	To configure your database partition: arcsight database pc

database pm

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

Examples	<code>arcsight database pm -cn Manage -m linux53_64_45sp3 -u admin -p arcsight</code>
-----------------	---

database xts

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

It is better to run this command locally on the machine that hosts the database. If you run it remotely, the wizard does not allow you to browse the remote directory and it cannot validate disk space availability before it expands the tablespace. If you run it locally it does both.

databasesetup

Description	Runs the ArcSight Database installer. This installer is documented in the "Installing ArcSight Database" chapter of the ESM Installation and Configuration Guide.
Applies to	Database
Syntax	<code>databasesetup</code>
Parameters	None
Examples	To run the database installation: <code>arcsight databasesetup</code>

dbcheck

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

dbview-generator

Description	Utility that generates database views based on the fields of a fieldset. Field sets are named subsets chosen from the available attributes of an event. To create a new field set or to see the existing ones, go to the Active Channels resource tree and click the Field Sets tab	
Applies to	Manager, Database	
Syntax	dbview-generator -f <fieldset> -m <manager> -n <view_name> -p <password> -u <user_name>	
Parameters	-f <fieldset>	URI of the fieldset from which you want to generate the database view
	-m <manager>	Name of the Manager
	-n <view_name>	Name for the view
	-u <user_name>	User name to connect to the Manager
	-p <password>	Password for the user_name
Examples	<p>To generate a database view containing fields in the Standard field set:</p> <pre>arcsight dbview-generator -f "/All Field Sets/ArcSight System/Active Channels/Standard" -m mymanager -n dv_view_standard -p mypassword -u myuser</pre> <p>To retrieve the data from the view you generated run the following command in SQL:</p> <pre>select * from db_view_standard</pre>	

deploylicense

Description	Install a new ArcSight license file. The Manager may be running; it detects the new license file automatically	
Applies to	Manager	
Syntax	deploylicense file	
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>To deploy a new license:</p> <pre>arcsight deploylicense</pre>	

downloadcertificate

Description	Wizard for importing certificates
--------------------	-----------------------------------

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

dropSLPartitions

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

exceptions

Description	Search for logged exceptions in ArcSight log files	
Applies to	Manager, Console, SmartConnectors	
Syntax	exceptions logfile_list [parameters] [path to the log file]	
	The path to the log file must be specified relative to the current working directory.	
Parameters	-x	Exclude exceptions/errors that contain the given string. Use @filename to load a list from a file.

-i	Include exceptions/errors that contain the given string. Use @filename to load a list from a file.
-r	Exclude errors.
-q	Quiet mode. Does not display exceptions/errors on the screen.
-e	Send exceptions/errors to the given email address.
-s	Use a non-default SMTP server. Default is bynari.sv.arcsight.com.
-u	Specify a mail subject line addition, that is, details in the log.
-n	Group exceptions for readability.
-l	Show only exceptions that have no explanation.
-p	Suppress the explanations for the exceptions.
Example	<p>To run:</p> <pre>arcsight exceptions /opt/home/arcsight/manager/logs/default/server.log*</pre>

export_system_tables

Description	Command to export your database tables. Upon successful completion the utility generates two files: a temporary parameter file and the actual database dump file, arcsight.dmp, which is placed in the Manager's <ARCSIGHT_HOME>/tmp .	
Applies to	Manager	
Syntax	<pre>export_system_tables <DBusername>/<DBpassword>@<Oracle_instance_name></pre>	
Parameters	<DBusername>	Database username
	<DBpassword>	Password for the database user
	<Oracle_instance_name>	Name specified in tnsnames.ora for the Oracle instance from which you are exporting the system tables
	-s	include session list tables

Examples	To run: <pre>arcsight export_system_tables <username>/<password>@<DBname></pre>
	<p>Note: When running the <code>export_system_tables</code> command, you may see a warning message in your command prompt or shell console window saying "Exporting questionable statistics". You can safely ignore this warning. This warning occurs when you export the table data with its related optimizer statistics and Oracle cannot verify the validity of these statistics.</p> <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	Wizard-like command to generate simple ArcSight FlexConnectors
Applies to	SmartConnectors
Syntax	<code>flexagentwizard</code>
Parameters	None
Examples	To run: <pre>arcsight flexagentwizard</pre>

groupconflictingassets

Description	Tool that groups asset resources with common attribute values. Group Conflicting Attribute Assets Tool. Assets can have conflicting IP addresses or host names within a zone	
Applies to	Manager	
Syntax	<code>groupconflictingassets</code>	
Parameters	<code>-c</code>	Clean (delete the contents of) the group to receive links to assets before starting. (Default: false)
	<code>-m <host></code>	Manager host name or address
	<code>-o <name></code>	Name for group to receive links to assets which have conflicting attributes. (Default: "CONFLICTING ASSETS")
	<code>-p <password></code>	Password
	<code>-port <n></code>	Port to connect to Manager (Default: 8443)
	<code>-prot <string></code>	Protocol { http https } (Default: https)
	<code>-u <name></code>	User name
	<code>-h</code>	Help

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

idefensesetup

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

import_system_tables

Description	Command to import database tables. The file you import from must be the one that export_system_tables utility created. This utility looks for the dump file, <code>arcsight_dump_system_tables.sql</code> , in the database's <code><ARCSIGHT_HOME></code> .	
Applies to	Manager, Database	
Syntax	<code>import_system_tables <old_user> <new_user> <password> <TNSname> <dump_file_path> <dump_file_name></code>	
Parameters	<code><old_user></code>	The database username that was used to export system tables using the <code>export_system_tables</code> command.
	<code><new_user></code>	The database username of the database to which you are importing system tables
	<code><password></code>	Password for <code><new_user></code>
	<code><TNSname></code>	Name specified in <code>tnsnames.ora</code> for the database to which you are importing the system tables
	<code><dump_file_path></code>	Absolute path or relative path from <code><ARCSIGHT_HOME></code>
	<code><dump_file_name></code>	Name of the dump file you plan to import

Examples	To run: arcsight import_system_tables <old_user> <new_user> <password> <TNSname> <dump_file_path> <dump_file_name>
	Note: Trend resources are exported, but not trend data from running them. After you import, re-run the trends to generate new data.

keytool

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

keytoolgui

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

kickbleep

Description	Runs a simple, standardized test using the bleep utility	
Applies to	Manager	
Syntax	kickbleep	
Parameters	-f	Properties file (silent mode)

	-g	Generate sample properties file
	-i	Mode: {swing, console, recorderui, silent} Default: swing
Examples	To run: arcsight kickbleep	

listsubjectdns

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

logfu

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

manager

Description	Runs the Manager in command line mode (not as a service)
Applies to	Manager
Syntax	manager
Parameters	None
Examples	To run the Manager: arcsight manager

managerinventory

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

manager-no-wrapper

Description	Run the Manager without automatic restart in case of fatal errors. (See manager for parameters.)
--------------------	--

Applies to	Manager
Syntax	manager-no-wrapper
Parameters	None
Examples	To run the manager without automatic restart: arcsight manager-no-wrapper

manager-reload-config

Description	Load the <code>server.defaults.properties</code> and <code>server.properties</code> files on the Manager	
Applies to	Manager	
Syntax	arcsight manager-reload-config	
Parameters	-diff	Displays the difference between the properties the Manager is currently using and the properties that this command loads
	-as	Forces the command to load properties that can be changed without restarting the Manager. The properties that require a Manager restart are updated in the <code>server.properties</code> but are not effective until the Manager is restarted
	-t <seconds>	Number of seconds after which the <code>manager-reload-config</code> command stops trying to load the updated properties file on the Manager
Examples	To reload config: arcsight manager-reload-config To view the differences between the properties the Manager is currently using and the properties that this command loads: arcsight manager-reload-config -diff	

managersetup

Description	Run the Manager Configuration Wizard	
Applies to	Manager	
Syntax	managersetup -i console	
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 managersetup	

managerstop

Description	Stop the Manager whether it is in service or command line mode
Applies to	Manager
Syntax	<code>managerstop</code>
Parameters	None
Examples	To stop the Manager service: <code>arcsight managerstop</code>

managersvc

Description	Start, stop, install, or uninstall the Manager as a service. Note: The start option does not work on Windows. To start Manager as a service on Windows, follow instructions in Chapter 1, Basic Administration Tasks , on page 9.
Applies to	Manager
Syntax	<code>managersvc {start stop restart status dump}</code>
Parameters	None
Examples	To start the Manager service (only on non-Windows platforms): <code>arcsight managersvc start</code>

managerthreaddump

Description	Script to dump the Manager's current threads
Applies to	Manager
Syntax	<code>managerthreaddump</code>
Parameters	None
Examples	To run: <code>arcsight managerthreaddump</code>

managerup

Description	Get the current state of the Manager. Returns 0 if the Manager is running and reachable. Returns 1 if not
Applies to	Manager
Syntax	<code>managerup</code>
Parameters	None

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

monitor

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

package

Description	<p>Import or export resources (users, rules, and so on) to or from one or more XML 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	<pre>package -action <action-to-be-taken> -package <package URI> -f <package-file></pre>																								
Parameters	<table> <tr> <td data-bbox="589 583 781 636">- action <action></td><td data-bbox="829 583 1317 716">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</td></tr> <tr> <td data-bbox="589 737 769 762">-config <file></td><td data-bbox="829 737 1313 789">The primary configuration file to use. Default is config/server.defaults.properties</td></tr> <tr> <td data-bbox="589 810 781 863">-convertbaseuri <baseuri></td><td data-bbox="829 810 1317 915">The base URI for packages that are converted from archives. This option is only used in conjunction with the -action convertarchives option</td></tr> <tr> <td data-bbox="589 936 704 961">-f <path></td><td data-bbox="829 936 1295 1041">The location of the package bundle file. File name paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME></td></tr> <tr> <td data-bbox="589 1062 743 1087">-m <manager></td><td data-bbox="829 1062 1198 1087">The Manager to communicate with</td></tr> <tr> <td data-bbox="589 1129 756 1155">-p <password></td><td data-bbox="829 1129 1317 1255">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.</td></tr> <tr> <td data-bbox="589 1276 756 1329">-package <packagerefs></td><td data-bbox="829 1276 1317 1381">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</td></tr> <tr> <td data-bbox="589 1402 781 1455">-pc <privateConfig></td><td data-bbox="829 1402 1255 1507">This configuration file overrides the server.defaults.properties file. The default location is config/server.properties</td></tr> <tr> <td data-bbox="589 1528 678 1554">-pkcs11</td><td data-bbox="829 1528 1313 1644">Use this option when authenticating with a PKCS#11 provider. For example, arcsight package -m <hostname> -pkcs11 -f <file path></td></tr> <tr> <td data-bbox="589 1665 743 1690">-port <port></td><td data-bbox="829 1665 1255 1717">The port to use for communication. The default port used is 8443</td></tr> <tr> <td data-bbox="589 1738 743 1791">-source <sourcefile></td><td data-bbox="829 1738 1284 1822">The source file. This is used in conjunction with the -f command which specifies an output file</td></tr> <tr> <td data-bbox="589 1843 756 1869">-u <username></td><td data-bbox="829 1843 1268 1896">The user name used for logging in to the Manager</td></tr> </table>	- 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 bundle file. File name paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME>	-m <manager>	The Manager to communicate with	-p <password>	The password with which to log in to the Manager. A password is not needed and not used in standalone mode, because the connection is made using the stored database account. Password is required otherwise.	-package <packagerefs>	The URI(s) of the package(s). This option is used in conjunction with -action install and -action uninstall in order to list which packages to operate upon	-pc <privateConfig>	This configuration file overrides the server.defaults.properties file. The default location is config/server.properties	-pkcs11	Use this option when authenticating with a PKCS#11 provider. For example, arcsight package -m <hostname> -pkcs11 -f <file path>	-port <port>	The port to use for communication. The default port used is 8443	-source <sourcefile>	The source file. This is used in conjunction with the -f command which specifies an output file	-u <username>	The user name used for logging in to the Manager
- 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 bundle file. File name paths can be absolute or relative. Relative paths are relative to <ARCSIGHT_HOME>																								
-m <manager>	The Manager to communicate with																								
-p <password>	The password with which to log in to the Manager. A password is not needed and not used in standalone mode, because the connection is made using the stored database account. Password is required otherwise.																								
-package <packagerefs>	The URI(s) of the package(s). This option is used in conjunction with -action install and -action uninstall in order to list which packages to operate upon																								
-pc <privateConfig>	This configuration file overrides the server.defaults.properties file. The default location is config/server.properties																								
-pkcs11	Use this option when authenticating with a PKCS#11 provider. For example, arcsight package -m <hostname> -pkcs11 -f <file path>																								
-port <port>	The port to use for communication. The default port used is 8443																								
-source <sourcefile>	The source file. This is used in conjunction with the -f command which specifies an output file																								
-u <username>	The user name used for logging in to the Manager																								

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

portinfo

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

querytuner

Description	<p>A troubleshooting tool that generates explain plans for all queries, and helps evaluate whether hints may improve the performance of some queries. This tool pulls explain plans for all the queries used by reports and trends and looks for ones that can execute inefficiently without database hints.</p> <p>All findings are logged in the file Manager's <ARCSIGHT_HOME>/logs/query-tuner.log.</p> <p>Run this tool from the Manager's bin directory either in a standalone mode (without the Manager running) or you can run it while the Manager is running.</p>										
Applies to	Database, Manager, Console										
Syntax	arcsight querytuner -m analyze -uri <uri_for_the_query>										
Parameters	<table> <tr> <td data-bbox="558 705 683 726">-m analyze</td><td data-bbox="829 705 1029 726">To analyze a query</td></tr> <tr> <td data-bbox="558 762 764 810">-d <query_duration></td><td data-bbox="829 762 1317 831">Optional parameter. query_duration is the time duration, for example, 1h, 2h, 1d, to be used while running the queries</td></tr> <tr> <td data-bbox="558 867 711 888">-t <timeout></td><td data-bbox="829 867 1317 989">Optional parameter. timeout is the number of seconds after which a slow running query will timeout. If you provide this value, performance is measured if and when a good hint is found</td></tr> <tr> <td data-bbox="558 1024 683 1045">-uri <uri></td><td data-bbox="829 1024 1300 1073">Optional parameter. uri is the URI of the query</td></tr> <tr> <td data-bbox="558 1108 586 1129">-h</td><td data-bbox="829 1108 1219 1146">Help for this command, for example, ./arcsight querytuner -h</td></tr> </table>	-m analyze	To analyze a query	-d <query_duration>	Optional parameter. query_duration is the time duration, for example, 1h, 2h, 1d, to be used while running the queries	-t <timeout>	Optional parameter. timeout is the number of seconds after which a slow running query will timeout. If you provide this value, performance is measured if and when a good hint is found	-uri <uri>	Optional parameter. uri is the URI of the query	-h	Help for this command, for example, ./arcsight querytuner -h
-m analyze	To analyze a query										
-d <query_duration>	Optional parameter. query_duration is the time duration, for example, 1h, 2h, 1d, to be used while running the queries										
-t <timeout>	Optional parameter. timeout is the number of seconds after which a slow running query will timeout. If you provide this value, performance is measured if and when a good hint is found										
-uri <uri>	Optional parameter. uri is the URI of the query										
-h	Help for this command, for example, ./arcsight querytuner -h										

Examples

To analyze all the queries

```
arcsight querytuner -m analyze
```

To analyze all queries and measure performance if a hint helps, -t is the timeout to be used while executing the query:

```
arcsight querytuner -m analyze -t 300000
```

To analyze a single query:

```
arcsight querytuner -m analyze -uri <uri_for_the_query>
```

For example,

```
arcsight querytuner -m analyze -uri "/All Queries/ArcSight
Foundation/Intrusion Monitoring/Executive Summaries/Business
Role/Business Role - Successful Attacks"
```

This tells you if any hint may potentially help. You should see the message "Hint that Helped=<the_actual_hint>" in the query-tuner.log file to look for a hint that might potentially help.

Open the query-tuner.log file. For every Query at the end of the query report look for the keyword "hasBadPattern=true" followed by "Hint that Helped=<the_actual_hint>" or sometimes you see "No hints could be found for this pattern."

Please contact Customer support when you see "hasBadPattern=true" followed by "No hints could be found for this pattern." Be prepared to provide the querytuner log and the package export of the query.

Once you run the Query Tuner tool and see that a hint has helped for a particular query, you can install the hint on the Manager from the

ArcSight Console. Refer to the Console's online help for information on how to do so.

Applying a Hint to a Query

Note: Please contact Customer Support before applying any hints received by running the Query Tuner.

Once you run the Query Tuner tool and see that a hint has helped for a particular query, you can add the hint to the query as follows:

- 1 In the Console's <ARCSIGHT_HOME>/current/config/console.properties file, set the following property:
`database.hint.editable=true`
- 2 Restart the Console if it is running.
- 3 Open the query-tuner.log file located in the Manager's <ARCSIGHT_HOME>/logs directory.
- 4 Scan through the file and locate the query URI. Copy the actual hint in the line "Hint that Helped=<the_actual_hint>" located below the query URI. Make sure not to copy the words "Hint that Helped="
- 5 In the ArcSight Console Navigator, open the **Reports** resource.
- 6 Click on the **Queries** tab to bring it forward.
- 7 Follow the URI for the query for which you want to apply the hint, right-click it and select **Edit Query**.
- 8 In the Inspect/Edit panel, paste the hint you copied in [Step 4](#) in the Database Hint box (the actual hint).

reenableuser

Description	Re-enable 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	Resource reference checker	
Applies to	Manager	
Syntax	refcheck	
Parameters	None	
Examples	To run: arcsight refcheck	

regex

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

replayfilegen

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

	<code>-i <mode></code>	Mode: console, silent, recorderui, swing
Examples	Run from the Console's <ARCSIGHT_HOME>/bin directory:	
	<code>arcsight replayfilegen</code>	
	To run in console mode:	
	<code>arcsight replayfilegen -i console</code>	

resetpwd

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

resvalidate

Description	Utility for checking 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.	
Applies to	Manager, Database	
Syntax	<code>resvalidate</code>	
Parameters	<code>-excludeTypes <exclude_resource_names></code>	Resource type to exclude from being checked; for example, Rule, DataMonitor If specifying multiple resource types to exclude, use comma to separate them. Resource type – Rule,DataMonitor(comma separated)
	<code>-out <output_dir></code>	Output directory for validation report. If none is specified, the report is placed in the directory from which you run the <code>resvalidate</code> command

`-persist [false | true]` 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 `resvalidate` command and `-persist=false`, the rule is reported as invalid but not marked invalid. However if `-persist=true`, the rule is marked as invalid.

Default: `persist=false`.

Examples To run, stop the Manager, then use:
`arcsight resvalidate`

ruledesc

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

runcertutil

Description	A wrapper launcher for the nss certutil tool used for managing certificates and key pairs. For more details on the certutil tool, you can visit the 'NSS Security Tools' page on the Mozilla website. 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.	
Applies to	N/A	
Syntax	<code>arcsight runcertutil</code>	
Parameters	<code>-A</code>	Add a certificate to the database
	<code>-a</code>	Use ASCII format or allow the use of ASCII format for input or output.

<code>-v <certificate_ validity_in_ months></code>	<p>Set the number of months for which a new certificate is valid. You can use this option with the</p> <p><code>-w</code> option which sets the beginning time for the certificate validity. If you do not use the <code>-w</code> option, the validity period begins at the current system time.</p> <p>If you do not specify the <code>-v</code> argument, the default validity period of the certificate is three months.</p>
<code>-w <beginning_ offset_months></code>	<p>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 (<code>-</code>) to indicate a negative offset. If this argument is not used, the validity period begins at the current system time.</p>
<code>-n <certificate_ name></code>	<p>Alias for the certificate</p> <p>Notes:</p> <ul style="list-style-type: none">• When generating a key pair on the Manager or ArcSight Web, it is mandatory to set the alias name to "mykey" (without the quotes)• When importing a certificate, you can set the alias name to any name of your choice
<code>-t <attributes></code>	<p>Set the certificate trust attributes</p>
<code>-d <certdb_dir></code>	<p>Specify the directory of the certificate database relative to <code><ARCSIGHT_HOME></code>.</p>
<code>-i</code>	<p>Certificate import request</p>
<code>-L</code>	<p>List all the certificates</p>
<code>-r</code>	<p>Encoding type</p>
<code>-o <filename></code>	<p>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.</p>
<code>-S</code>	<p>Create a certificate to be added to the database</p>
<code>-s <subject></code>	<p>Subject name</p>
<code>-k <key_type></code>	<p>Type of key pair to generate</p>
<code>-x</code>	<p>Self signed</p>
<code>-m <serial_number></code>	<p>Certificate serial number</p>
<code>-v <days></code>	<p>Validity period in days, for example, use</p> <p><code>-v 1825</code></p> <p>to change the validity period to 5 years where 1825 is the number of days in 5 years.</p>

	-V	Check the validity of the certificate
	-n <cert_name>	Certificate name
	-H	Help on this tool
Examples	To run: arcsight runcertutil	

runmodutil

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

runpk12util

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

script

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

searchindex

Description	Utility that creates or updates the search index for resources. If you provide the credentials for the Manager, it automatically associates with the newly created or updated index. However, if you do not specify any credentials, you have to manually configure the Manager to use the updated index. Note: Supporting 50,000 actors requires a minimum of 2 GB heap size for this service. The value of the heap size needs to be modified in <ARCSIGHT_HOME>/bin/scripts/searchindex.bat and <ARCSIGHT_HOME>/bin/scripts/searchindex.sh files. The default value in these files is set to 1028m.	
Applies to	Manager	
Syntax	searchindex -a action	
Parameters	-a <action>	Possible actions: create, update, or regularupdate create—Creates a new search index. update—Updates all resources in the index that were touched since the last daily update was run. Although “update” is a scheduled task that runs daily, you can run it manually. regularupdate—Updates all resources in the index that were touched since the last regular update was run. Although “regular update” is a scheduled task that runs every 5 minutes, you can run it manually.
	-m <manager>	Name of the Manager
	-p <password>	Password for the user
	-t <time>	Time stamp that indicates starting when the resources should be updated
	-u <user>	User name with which to log in to the Manager
Examples	To run: arcsight searchindex -a <action>	

sendlogs

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

tee

Description	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 sslinfo.txt	

tempca

Description	Inspect and manage demo certificates	
Applies to	Console	
Syntax	tempca	
Parameters	-a <alias>	Key store alias of the private key to dump
	-ac	Add the demo CA's certificate to the client truststore
	-ap	Create demo SSL key pair and add it to the Manager key store
	-dc	Dump/export the demo CA's certificate to a file (demo.crt) for browser import
	-dpriv	Dump private key from the Manager key store

-f <file>	Filename to write the demo CA's certificate to
-i	Display summary of current SSL settings
-k <n>	Key store: Manager (1) or Web Server (2)
-n <host>	Host name of the Manager (opt for the creation of a demo key pair)
-nc	No chain: Do not include certificate chain (option for creation of a demo key pair)
-rc	Reconfigure not to trust demo certificates. Removes the demo CA's certificate from the client truststore
-rp	Remove pair's current key pair from the Manager key store
-v <days>	Validity of the new demo certificate in days (Default: 365)
Examples	To run: arcsight tempca

testdbconnection

Description	Test whether the database is up and running	
Applies to	Manager, Database	
Syntax	testdbconnection -u username -p password	
Parameters	-u <username>	(Required) User name of the Arcsight user in the database. Typically, arcsight
	-p <password>	(Required) Password of the ArcSight user in the database
	-i <instance>	Instance of the database. Default: arcsight
	-p <port>	Port to connect. Default: 1521
	-s <host>	Hostname of the machine on which database is located. Default: localhost
	-t <dbtype>	Database type: oracle. Default: oracle
Examples	arcsight testdbconnection -u arcsight -p password	

threaddumps

Description	Utility to extract and reformat thread dumps from the specified Manager log file
Applies to	Manager

Syntax	threaddumps <file>	
Parameters	<filename>	Specify the name of a log file.
	-h	Display command help
Examples	To run: arcsight threaddumps	

tproc

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

uninstallservice

Description	Wizard to uninstall service	
Applies to	Manager, ArcSight Web	
Syntax	uninstallservice	
Parameters	-c <component>	Component whose service is to be uninstalled—Manager or Web
Examples	To run: arcsight uninstallservice	

webserver

Description	Start the ArcSight Web server	
Applies to	ArcSight Web	
Syntax	webserver	
Parameters	-c <file>	Base configuration file
	-host <host>	Manager name or address
	-p <port>	Manager port
	-pc <file>	User configuration file
Examples	To start the ArcSight Web server: arcsight webserver	

webserver-no-wrapper

Description	Start the ArcSight Web server without automatic restart		
Applies to	ArcSight Web		
Syntax	webserver-no-wrapper		
Parameters	-ms <mem>	Minimum memory	
	-mx <mem>	Maximum memory	
Examples	To start the ArcSight Web server without automatic restart: arcsight webserver-no-wrapper		

webserversetup

Description	See runwebsetup and websetup		
Applies to	ArcSight Web		

webserversvc

Description	Start, stop, restart, or install the ArcSight Web server as a service		
Applies to	ArcSight Web		
Syntax	webserversvc [parameters]		
	You can use the single letter parameters shown in brackets instead of entering the whole word on Windows only		
Parameters	Description	Windows	Unix

start or (-s)	Start the service	No (Command available but does not work)	Yes
stop or (-q)	Stop the service	Yes	Yes
restart	Restart the service	No	Yes
status	Check status of service	No	No
install or (-i) <initialHeap> <maxHeap>	Install the service Optional parameters: <code>initialHeap</code> —Initial heap memory size, in MB. (Default: 128) <code>maxHeap</code> —Maximum heap memory size, in MB. (Default: 512)	Yes	No
remove or (-r)	Remove the service	Yes	No
console or (-c)	Console Mode	Yes	No
Examples	To start the ArcSight Web server as a service: <code>arcsight webserver svc start</code>		

websetup

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

whois

Description	Script used by the <code>whois</code> command of the console		
Applies to	Console		
Syntax	<code>whois [-p <port>] [-s <host>] <target></code>		
Parameters	<code>-p <port></code>	Server port	
	<code>-s <host></code>	Name or address of 'whois' server	

	<target>	Name or address to lookup
Examples	To run: arcsight whois	

Appendix B

Troubleshooting

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

If you intend to have Customer Support guide you through a diagnostic process, please prepare to provide specific symptoms and configuration information. If you intend to do the initial diagnostic steps yourself, proceed through the following checklist systematically, trying each applicable item and noting the results for reference.

This appendix is divided into the following sections:

[“General” on page 161](#)
[“Query and Trend Performance Tuning” on page 164](#)
[“SmartConnectors” on page 167](#)
[“ArcSight Console” on page 168](#)
[“Manager” on page 170](#)
[“ArcSight Web” on page 171](#)
[“Database” on page 172](#)
[“SSL” on page 173](#)

General

Report is empty or missing information.

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

Running a large report crashes the Manager.

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the 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.canarchiveportinseparateprocess=true`. (This makes a new report parameter available on the Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight Console, open the report that you want to run in a separate process in the Report Editor, and click the **Parameters** tab. Set the parameter **Generate Report In Separate Process** to `true`.
- 4 Run the report. The report should run like a normal report, but it does not consume the resources of the Manager 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>
```

Reports that query over a large time range with complex joins take a long time to run.

You can expedite a report that queries over a large time range with complex joins if you set it to query with a full scan database hint. To set the query with full scan database hint, do this:

- 1 On the Manager in the `server.properties` file, set `report.canquerywithfullscanhint=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 contain the full scan hint in the Report Editor, and click the **Parameters** tab. Set the parameter **Query with Full Scan Hint** to `true`.

4 Run the report.



- 1 Use this parameter only in special circumstances if your organization has determined with the help of Customer Support or professional services that it is appropriate.
- 2 If a report is saved with the parameter set to "true", the full database optimization hint is applied even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to false later on.
- 3 When the property `report.canquerywithfullscanhint` is set to "true", the report uses the `FULL_SCAN` hint in the SQL queries it generates to query the database. The content of the report does not change, but the queries logged in `server.report.log` contain the hint. The main benefit of querying the database with the `FULL_SCAN` hint is that it can significantly reduce the runtime for SQL queries that query over events within a large time range and contain complex joins.

Some Asian language fonts appear mangled when generating reports in PDF

This problem occurs because some Asian language fonts that are truetype fonts are not supported directly by versions of Adobe Reader earlier than version 8.0. In order to work around this, each truetype font must be mapped to an opentype font supported in Adobe Reader 8.0. ArcSight provides this mapping in the

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

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

- 1 Install a localized Adobe Reader 8.0 depending on the language of your platform on your Manager machine. This version of the Adobe Reader installs the opentype fonts by default.
- 2 Edit the `server.properties` file as follows:
 - a Set `report.font.truetype.path` property to point to the directory that contains the truetype and opentype font. On Windows it is typically `C:\WINNT\fonts;C:\Program Files\Adobe\Reader 8.0\Resource\CIDFont` where ";" is used as a path separator to separate the multiple paths. Use ":" as a path separator in Unix. On Unix platforms, the truetype font path may differ depending on the specific Unix platform, but it is typically `/usr/lib/font`. The CIDFont directory is always the same relative to the Adobe Reader installed directory. So, the default directory would be `/usr/lib/font:<adobe_reader_dir>/Resource/CIDFont`.
 - b Set `report.font.cmap.path` property to point to Adobe Reader's CMap directory. On windows, it is typically `C:\Program Files\Adobe\Reader 8.0\Resource\CMap`. On Unix, the CMap path is relative to the Adobe Reader installation -- `<adobe_reader_dir>/Resource/CMap`.

E-mail notification doesn't happen.

If you receive the following error:

```
[2009-12-03 14:31:33,890] [WARN
] [default.com.arcsight.notification.NotifierBase] [send] Unable to
```

send out e-mail notification, notifications have not been configured.

- Verify the following properties are set in the `server.properties` file:
`notifications.enable=true`

and
`notifications.incoming.enable=true`
- Check `server.properties` file to find which SMTP server is associated with the Manager. Make sure that the SMTP server is up and running.

Review the Notification resource and confirm the e-mail address and other configuration settings.

Notification always escalates.

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

Pager notification doesn't happen.

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

Query or report performance degrades suddenly.

- Check that the ArcSight Database host has sufficient disk space.
- Check that the ArcSight Database statistics are up to date.
- Has the network infrastructure changed?
- Has the ArcSight Database or DBMS configuration changed?

See also, [“Query and Trend Performance Tuning” on page 164](#) for more information on performance enhancements and suggestions on how to improve performance with regard to queries and trends.

Query and Trend Performance Tuning

To improve query execution in high-EPS systems, various queries used by the trends in the default ArcSight 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.

Persistent Database Hints

Database hints are provided in system content packages. These hints are not visible in the Console. Please do not attempt to modify the system queries through the Console because this causes the hint to disappear and the query to run slowly again.

server.defaults.properties Entries for Trends

- `trends.query.timeout.seconds=7200`

This is the amount of time that a trend query is allowed to run, in seconds, before the SQL statement times out and the trend query fails. If absent or 0, no time-based timeout is applied.

- `trends.query.timeout.percent=50`

This is the amount of time that a trend query is allowed to run, as a percentage of the query interval for interval trends, before the SQL statement times out and the trend query fails. If absent or 0, no percentage-based timeout is applied.

As an example, with a 50 percent setting, a query covering a start/end time range of 1 hour times out after 30 minutes. A start/end time range covering 1 day would time out after 12 hours.

If both timeouts are specified, the system uses the smaller of the two.

- `trends.query.failures.deactivation.threshold=3`

If this many consecutive “accumulate” (not refresh) runs fail for any reason, the system automatically disables the trend. The check is always performed after any accumulate query run fails. Once the threshold is reached, any remaining queries to be executed by this task are skipped. If this setting is absent or 0, the checking mechanism is turned off.

If a trend or query is stopped because of any of the above reasons, an audit event reflects this.

Troubleshooting Checklist after Restarting the Manager

- Use the Console Trend Editor to manually disable any trends that you do not need or that you notice have excessive query times. Disabling these trends helps reduce scheduler and database contention.
- Your own custom trends may have long-running queries and may be timing out. If this is the case, use the Query Tuner tool provided with this patch. See the description on query tuner in the ArcSight Commands appendix for instructions on how to use this tool. Once you have identified a hint that might help, please contact Customer Support and provide a package with your query or queries for ArcSight to examine. We investigate and determine if database hints can improve your trend queries.
- As trend data gathering tasks wake up, the trend attempts to fill in the gaps for missing intervals. Depending on the size of the gaps, this may take some time before the trends catch up.
- A trend does not usually re-run any previously failed runs. If you want to re-run a particular time, you need to manually request it from the Trend Editor.

Disable these Trends on High Throughput Systems

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

```
/All Trends/ArcSight Administration/ESM/User Access/ArcSight User Login Trends - Hourly
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/Asset Configuration Change Tracking/Host Configuration Modifications
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/Asset Restarts/Asset Startup and Shutdown Events - Daily Trend
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/User  
Account Modifications/User Account Creation
```

```
/All Trends/ArcSight Foundation/Configuration Monitoring/User  
Account Modifications/User Account Modifications
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Reconnaissance/Port Scanning
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Reconnaissance/Zone Scanning Events by Priority
```

```
/All Trends/ArcSight Foundation/Intrusion Monitoring/Operational  
Summaries/Vulnerability View/Prioritized Vulnerability Events by  
Zone
```

```
/All Trends/ArcSight Foundation/Network Monitoring/Overall Traffic
```

How 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 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).

Enhancing the Performance Globally for all Database Queries

You can enhance the performance for all queries made against the database. When Oracle Optimizer decides on a query execution plan, it can dynamically do a sampling of actual data to estimate the cost of the query. Based on the findings of this sampling, the Optimizer comes up with the best query execution plan which helps improve query performance. To enable dynamic sampling, run:

```
% arcdbutil sql
```

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

```
SQL> @<ARCSIGHT_HOME>\utilities\database\oracle\common\sql\
```

```
SetDynamicSampling.sql
```

In addition to Dynamic Sampling, you can update the IO transfer speed in the database which helps in query performance. If you do not update the IO transfer speed, Oracle defaults to a very low IO transfer speed estimate that adversely affects the query execution plan. Run the following command (while logged in as sysdba):

```
SQL> @ARCSIGHT_HOME\utilities\database\oracle\common\sql\
```

```
GatherSystemStats.sql
```

This script should also be run every time you make any storage hardware changes that affects IO transfer speeds.

Unable to Execute Query: ORA-01555

If you have too many long-running queries, you might get an error that looks like this:

```
ORA-01555: snapshot too old: rollback segment number 24 with name
"_SYSSMU24_4040026624$" too small
```

If this occurs, enlarge the ARC_UNDO tablespace incrementally until you get satisfactory results.

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.

Partition Archiver problems.

See Partition Archiver under [“Database” on page 172](#).

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 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.

This can happen when you open many independent viewing channels. If you need to do this often, change the memory settings in the `console.bat` or `console.sh` file. Find the line that starts `set ARCSIGHT_JVM_OPTIONS=` and change the parameter `-Xmx128m` to `-Xmx256m`. You must restart the Console for the new setting to take effect.

Acknowledgement button is not enabled.

The Acknowledgement button is enabled when there are notifications to be acknowledged and they are associated with a destination that refers to the current user. To enable the button, add the current user to the notification destination.

The grid view of Live security events is not visible.

To restore the standard grid view of current security events, select **Active Channels** from the Navigator drop-down menu. Double-click **Live**, found at `/Active channels/Shared/All Active channels/ArcSight System/Core/Live`

The Navigator panel is not visible.

Press **Ctrl+1** to force the Navigator panel to appear.

The Viewer panel is not visible.

Press **Ctrl+2** to force the Viewer panel to appear.

The Inspect/Edit panel is not visible.

Press **Ctrl+3** to force the Inspect/Edit panel to appear.

Internal ArcSight events appear.

Internal ArcSight events appear to warn users of situations such as low disk space for the ArcSight Database. If you are not sure how to respond to a warning message, contact Customer Support.

The Manager Status Monitor reports an error.

The Console monitors the health of the Manager and the ArcSight Database. If a warning or an error occurs, the Console may present sufficient detail for you to solve the problem. If not, report the specific message to Customer Support.

Console logs out by itself.

Check the Console log file for any errors. Log in to the Console. If the Console logs out again, report the error to Customer Support.

Console stops responding when sending a test SNPP notification.

If the Console stops responding when sending a test SNPP notification, it may indicate that the SNPP port is blocked by a firewall or packet filtering device.

Cannot log in to ArcSight Web from within the Console.

In ArcSight Console, if you click **File->Launch** ArcSight Web, it starts the browser within the Console window and display the ArcSight Web login screen. Once you enter your user name and password for the Manager, you should be able to log into the Web from within the Console. However, if in spite of entering the correct login information, you cannot login to ArcSight Web and your browser appears to hang, then you have to change the security settings on your browser. To do so on Internet Explorer:

- 1 Go to **Tools->Internet Options**.
- 2 Click the **Security** tab.
- 3 Click the **Internet** icon.
- 4 Click the **Custom level...** button.
- 5 Select **Medium** from the **Reset to** drop down menu.
- 6 Click **Reset** button. You receive a warning asking you whether you want to change the security setting of the zone. Click **Yes**.
- 7 Click **OK** in the Security Options box.
- 8 Click **OK** in the Internet Options box.

- 9 Go back to the Console and try to restart ArcSight Web from within the Console by clicking **File->Launch ArcSight Web**.

Console does not start in Windows 2008

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

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`.

To check database connectivity manually, open a command window on

`<ARCSIGHT_HOME>/bin` (on the Manager host) and run:

```
arcsight testdbconnection
```

Manager shuts down.

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

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

For example, the following error indicates that a connection cannot be established with the underlying Oracle DBMS:

```
[ERROR] [default.com.arcsight.common.persist.oracle.OracleDatabaseInfoBroker] [getDatabaseInfo]
```

```
com.arcsight.common.persist.PersistenceException: Unable to get connection: Io exception: Connection reset by peer: socket write error
```

This indicates that the Oracle TNS Listener is running but the actual ArcSight Database service is not reachable.

Manager restarts automatically.

If the Java Virtual Machine (JVM) fails to respond within two minutes, an ArcSight watchdog program automatically restarts it, which reduces system performance but does not cause data loss. This situation has been observed on low-end Windows-based host machines with page file size optimization enabled. Optimization complicates the garbage collection process, rendering the JVM non-responsive for longer than two minutes.

Disable page file size optimization. Perform the following steps to disable page file size optimization on Windows 2000 Manager hosts:

- 1 Right-click **My Computer** and select **Properties** from the menu. Select the **Advanced** tab.
- 2 Click **Performance Options** for Windows 2000.

- 3 Set **Initial size** to the same value as **Maximum size**.
- 4 Click **Set**.
- 5 Click **OK**.

The log contains a warning “Side table for [name] is 100% full. System performance will be affected.”

This log error message is the result of the default sizes for side object caches being too small for some larger production deployments. Although system performance is generally not affected, to stop generating the warning message, add the following lines to the `server.properties` file and restart the Manager:

```
persist.securityevent.stcache.GeoDescriptor=50000
persist.securityevent.stcache.AgentDescriptor=500
persist.securityevent.stcache.DeviceDescriptor=50000
persist.securityevent.stcache.CategoryDescriptor=3000
persist.securityevent.stcache.LabelsDescriptor=2000
persist.securityevent.stcache.ResourceRef=20000
```

If you continue to see the error message after this change, one or more SmartConnectors may be configured incorrectly. Contact HP Customer Support.

Scheduled Task Run is Off When Switching from Daylight Savings Time to Standard Time or Vice Versa.

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

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

ArcSight Web

Some content, particularly dashboards, is not visible.

Install the latest Adobe Flash plug-in to your browser. Visit the Adobe web site to download this free plug-in.

Can't log in to ArcSight Web.

Check that the ArcSight Web Server is up and running. If ArcSight Web is up, check that the Manager is also up and running.

If the Manager is running, but you still can't log in, suspect any recent network changes, such as the installation of a firewall that affects communication between the ArcSight Web server and the Manager host.

If you can log in to the ArcSight Console but not ArcSight Web, focus on any recent network changes and any configuration changes to your browser.

Make sure that the version number of ArcSight Web matches that of the Manager. If the version numbers do not match, log in is disabled.

Can't start ArcSight Web.

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

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

Database

Partition Archiver can't connect to Manager.

Check the Partition Archiver log for errors. The log file is found in the logs directory:

```
<ARCSIGHT_HOME>/logs/default/agent.out.wrapper.log
```

An SSL Handshake exception in the log indicates a problem with the Manager's certificate. From the SmartConnector's install directory, run the following command to establish a valid certificate:

```
./arcsight agent tempca -ac
```

Oracle hangs without warning.

If automatic archive log mode is turned on, Oracle hangs if the archive log destination becomes full. Oracle resumes when you make archive log space available.

An e-mail notification reports a problem with the ArcSight Database.

Don't ignore a warning or error notification from the ArcSight system. If the message is not clear to you, contact Customer Support. Ignoring a database error can lead to the Manager suddenly stopping, which eventually leads to security event data loss.

See Appendix C, Monitoring Database Attributes, for more information.

Partition logs may not be complete.

Only one duplicate log file can be written to at one time. Therefore, if a partition utility is in progress and another partition utility starts in parallel, the logs for the first utility are no longer written to the duplicate log file. However, the log data for the first utility is not lost; it is available in the <ARCSIGHT_HOME>/logs/server.log file.

See the "Database Administration" chapter, for more information.

SSL

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

Causes:

The SSL server may not be running.

- A firewall may be preventing connections to the server.

Resolutions:

- Ensure that the SSL server is running.
- Also, ensure that a firewall is not blocking connections to the server.

Cannot connect to the SSL server

The hostname to which the client initiates an SSL connection should exactly match the hostname specified in the server SSL certificate that the server sends to the client during the SSL handshake.

Causes:

- You may be specifying Fully Qualified Domain Name (FQDN) when only hostname is expected or the other way around.
- You may be specifying IP address when hostname is expected.

Resolutions:

- Type exactly what the server reports on startup in `server.std.log` ("Accepting connections at `http://...`")
- For Network Address Translation (NAT) or multi-homed deployments, use hosts file to point client to correct IP.

PKIX exchange failed/could not establish trust chain

Cause:

Issuer cannot be found in trust store, the cacerts file.

Resolution:

Import issuer's certificate (chain) into the trust store.

Issuer certificate expired

Cause:

The certificate that the SSL server is presenting to the client has expired.

Resolution:

Import the latest issuer's certificate (chain) into the trust store.

Cannot connect to the Manager: Exception in the server log

Cause:

If you replaced the Manager's key store, it is likely that the old key store password does not match the new password.

Resolution:

Make sure the password of the new key store matches the old key store. If you do not remember the current key store's password, run the Manager Configuration Wizard on the Manager (ArcSight Web Configuration Wizard on the Web) to set the password of the current key store to match the new key store's password.

Certificate is invalid

Cause:

The timestamp on the client machine might be out of the bounds of the validity range specified on the certificate.

Resolution:

Make sure that the current time on the client machine is within the validity range on the certificate. To check the certificate's valid date range see ["Viewing Certificate Details" on page 43](#).

Issue with Internet Explorer and ArcSight Web in FIPS Mode

When using Internet Explorer (IE) with ArcSight Web running in FIPS mode, IE may return an error message when you attempt to log in using user name and password authentication:

- ArcSight Web is FIPS-enabled
- You have opted to use Password Based or SSL Client Based Authentication
- You use ActivClient middleware and have registered the certificate from Smart Card into Internet Explorer
- You have enabled TLS v1 on Internet Explorer
- ArcSight Web's truststore contains the Smart Card issuer's certificate
- The card is not present in the card reader

This is an issue with Internet Explorer. To use the password based authentication in FIPS 140-2 mode, you need to remove all registered PKCS#11 related certificates from the Internet Explorer certificate repository. To do so:

- 1** Go to **Tools->Internet Options** and click the **Content** tab.
- 2** Click **Certificates** and then select the **Personal** tab.
- 3** Select all the PKCS#11 related certificates and click **Remove**.
- 4** Click **Intermediate Certification Authorities**.
- 5** Select all the PKCS#11 related certificates and click **Remove**.

Appendix C

Monitoring Database Attributes

This chapter provides information about in-built checks that monitor database attributes and generate warning or error messages, as appropriate. This appendix is divided into the following sections:

[“Understanding Database Checks” on page 177](#)

[“Disabling Database Checks” on page 178](#)

[“List of Database Check Tasks” on page 179](#)

Understanding Database Checks

ESM provides in-built checks to monitor database configurations and runtime attributes. These checks inform you if attributes such as Oracle account password or available reserve partitions drop below an acceptable value. Depending on the severity of deviation, a warning or an error message is generated.

If an error or a warning message is generated, these actions take place:

- A message is logged to the `server.std.log` file on the Manager.
- If you have configured the Manager to generate e-mail, a message is sent.
- A notification message is displayed on the ArcSight Console.

If an error message is generated, the event flow to the Manager is stopped. In that case, SmartConnectors start caching the events so there is no loss of events. After you have resolved the issue that caused the error, you can click a reactivation URL that is included in the error message to restart the event flow.

Each check task is scheduled to run at a predefined interval and compare the current system state with a predefined threshold, both of which can be changed to suit your needs.

The `server.defaults.properties` defines the interval and threshold for each task. You can override these values in the `server.properties` file on the Manager. That is, do not edit the `server.defaults.properties` file. Copy the entry to the `server.properties` file and then change the setting.

Message text

The following is an example of the error or warning e-mail message that is sent:

```
Date: Fri, 16 Dec 2011 01:24:36 +0000 (GMT+00:00)
To: administrator@mycompany.com
```

```
[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 1.0K --]

== SUBSYSTEM STATUS CHANGED =====

Error - Event Receiver

== ORIGIN OF CHANGE =====

Error - PartitionManagerCheckTaskTracker

-- DESCRIPTION -----

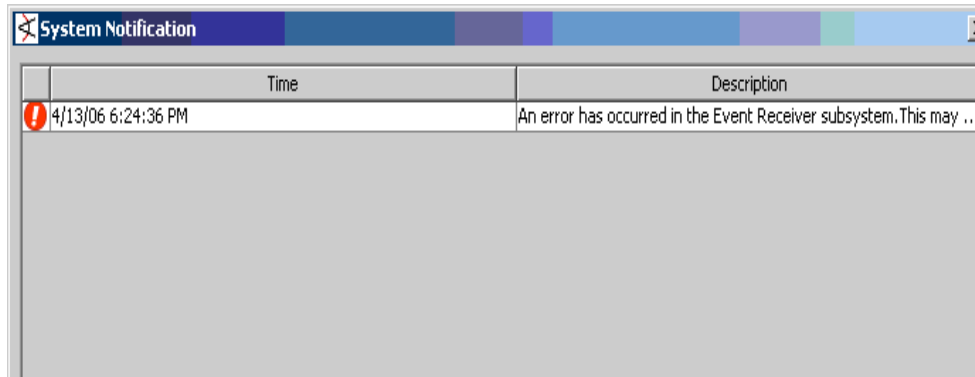
[PartitionManagerCheckTaskTracker: Fatal Error: There are only 0
of 7 reserve partitions available. This is likely due to failures
in Partition Manager runs for the past few days. If this situation
is not fixed, the MAX partition will become the CURRENT partition
in the next few days, causing system failure.

Check the Partition Manager logs for errors and fix the problem
before proceeding.

Fix the root cause of the error reported. If the event flow is
stopped, use the

following URL to resume:
https://yourmanager.mycompany.com:8443/arcsight/web/reactivate.jsp
?id=87160D7E0425A22FBE5354FE90387A96]
```

The following is an example of the notification message that is displayed on the Console:



Disabling Database Checks

If you do not want to run a specific database check, you can disable it.

To disable a database check task, specify the name of the check task as the value for the `whine.check.exclude` property in the `server.properties` file on the Manager.



To obtain the name of a task, see List of Database Check Tasks.

For example, to exclude `PartitionManagerCheckTask`, enter this in the `server.properties` file:

```
whine.check.exclude=PartitionManagerCheckTask
```

To exclude multiple check tasks, specify a comma-separated list for the `whine.check.exclude` property; for example,

```
whine.check.exclude=PartitionManagerCheckTask,
PartitionCompressorCheckTask
```

List of Database Check Tasks

The following is a list of check tasks available in this ESM release. Each check task includes an interval at which that task is performed, any attributes that are checked, and the default thresholds at which a Warning or Error message is generated.

1 General check tasks

```
# The default interval to run configured check tasks, in seconds.
```

```
whine.check.interval=30
```

```
# Specific check intervals for checking free space, in seconds.
```

```
whine.check.interval.DBFreeSpaceChecker=30
```

```
# The actual update interval of free database space information by
DatabaseInfoBroker, seconds.
```

```
databaseinfo.update.interval=30
```

2 AccountCheckTask - Checks User Account Expiry

```
# AccountCheckTask is run every 12 hours
```

```
whine.check.interval.AccountCheckTask=43200
```

```
# AccountCheck Password Expiry warning threshold (days)
```

```
dbcheck.oracle.account.warn.threshold=5
```

```
# AccountCheck Password Expiry error threshold (days)
```

```
dbcheck.oracle.account.error.threshold=2
```

3 ArchiveDestinationCheckTask - If the redo log archive destination is cross mounted in the manager box, this task checks for space availability in such a destination

```
# ArchiveDestinationCheckTask is run every 1 hour
```

```
whine.check.interval.ArchiveDestinationCheckTask=3600
```

```
# Whether database archive destination file systems are cross-mounted in the
Manager box
```

```
dbcheck.oracle.archivedest.xmount=false
```

```
# Minimum number of hours of archive space that should be available
```

```
dbcheck.oracle.archivedest.threshold.hours=18
```

4 ArchiveSessionCheckTask - Checks whether any Oracle sessions are stuck on "archive required" wait event.

```
# ArchiveSessionCheckTask is run every 30 seconds
```

```
whine.check.interval.ArchiveSessionCheckTask=30
```

5 ParameterCheckTask - Checks default and non-default Oracle parameters against values specified below.

```
# ParameterCheckTask is run every 24 hours
```

```
whine.check.interval.ParameterCheckTask=86400
```

```
# Suggested % of shared_pool in terms of total sga
dbcheck.oracle.parameter.sharedpool=20

# Suggested % of db_cache in terms of total sga
dbcheck.oracle.parameter.dbcache=40

# Suggested minimum db_files value
dbcheck.oracle.parameter.dbfiles=200

# Suggested maximum java_pool size
dbcheck.oracle.parameter.javapool=0

# Suggested minimum log_buffer size
dbcheck.oracle.parameter.logbuffer=1048576

# Suggested maximum parallel_max_servers value
dbcheck.oracle.parameter.parallelmaxservers=0

# Suggested pga_aggregate_target value
dbcheck.oracle.parameter.pgaaggreatarget=40

# Suggested minimum processes value
dbcheck.oracle.parameter.processes=100

# Suggested minimum undo_retention value
dbcheck.oracle.parameter.undoretention=43200

# Suggested timed_statistics value
dbcheck.oracle.parameter.timedstatistics=TRUE

# Suggested workarea_size_policy value
dbcheck.oracle.parameter.workareasizepolicy=AUTO

# Specific check intervals for certian tasks, in seconds
whine.check.interval.DBFreeSpaceChecker=10

# Suggested filesystemio_options parameter value
dbcheck.oracle.parameter.filesystemiooptions=SETALL
```

- 6 PartitionArchiverCheckTask** - Checks whether partition archiver is working successfully.

```
# PartitionArchiverCheckTask is run every 12 hours
whine.check.interval.PartitionArchiverCheckTask=43200

# Archiver Lag Warning Threshold
dbcheck.oracle.archiver.warnthreshold=2
```

- 7 PartitionCompressorCheckTask** - Checks whether partition compressor is working successfully.

```
# PartitionCompressorCheckTask is run every 12 hours
whine.check.interval.PartitionCompressorCheckTask=43200
```

- 8 PartitionManagerCheckTask** - Checks whether enough reserve partitions are available.

```
# PartitionManagerCheckTask is run every 12 hours
whine.check.interval.PartitionManagerCheckTask=43200

# Partition Manager Warning Threshold (# of available reserve partitions)
dbcheck.oracle.manager.warnthreshold=5
```

Partition Manager Error Threshold (# of available reserve partitions)
`dbcheck.oracle.manager.errorthreshold=2`

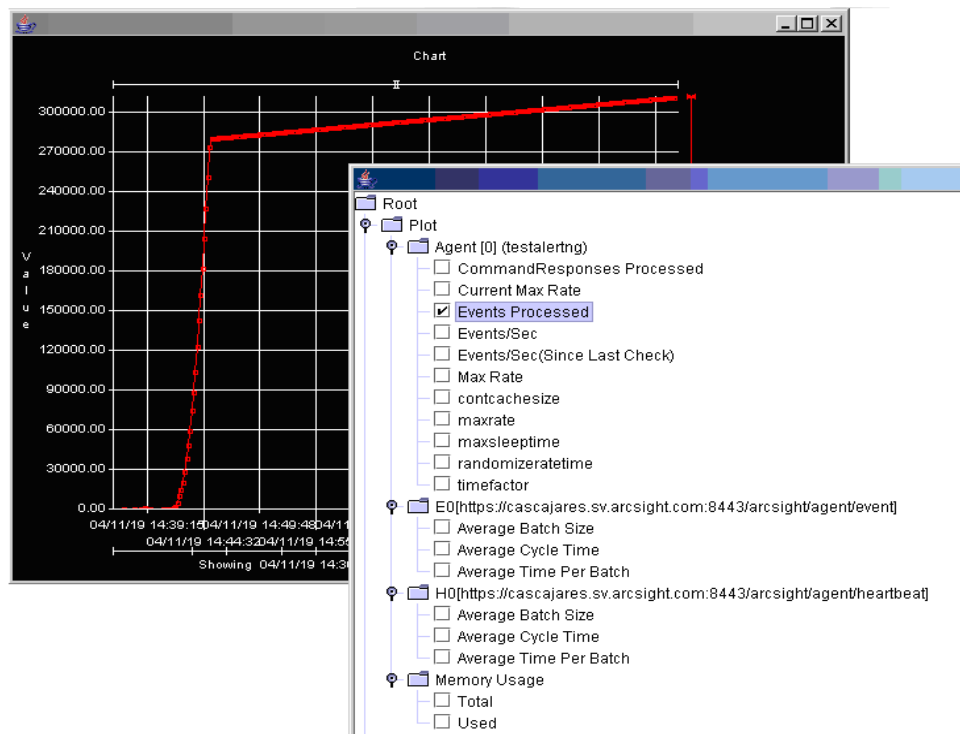
Appendix D

The Logfu Utility

This appendix is divided into the following sections:

- [“Running Logfu” on page 184](#)
- [“Example” on page 186](#)
- [“Troubleshooting” on page 186](#)
- [“Menu” on page 188](#)
- [“Typical Data Attributes” on page 188](#)
- [“Intervals” on page 189](#)

Logfu is an ArcSight utility that analyzes log files. It is indispensable for troubleshooting problems that would otherwise require poring over text logs. Logfu generates an HTML report (`logfu.html`) and, especially in SmartConnector mode, includes a powerful graphic view of time-based log data. Logfu pinpoints the time of the problem and often the cause as well.



Logfu has two windows: the interactive Chart and the Plot/Event window.

Running Logfu

Logfu finds log files in the current directory. The `-a` or `-m` switches tell it which file names to look for. The `-m` switch tells it to look for all three Manager logs—`server.std.log`, `server.log`, and `server.status.log`—for example.

To run Logfu, follow these steps:

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

For Manager logs, run: `../bin/arcsight logfu -m`

For SmartConnector logs, run: `../bin/arcsight agent logfu -a`
- 3 Right-click in the grid and select **Show Plot/Event Window** from the context menu.
- 4 Check at least one attribute (such as Events Processed) to be displayed.

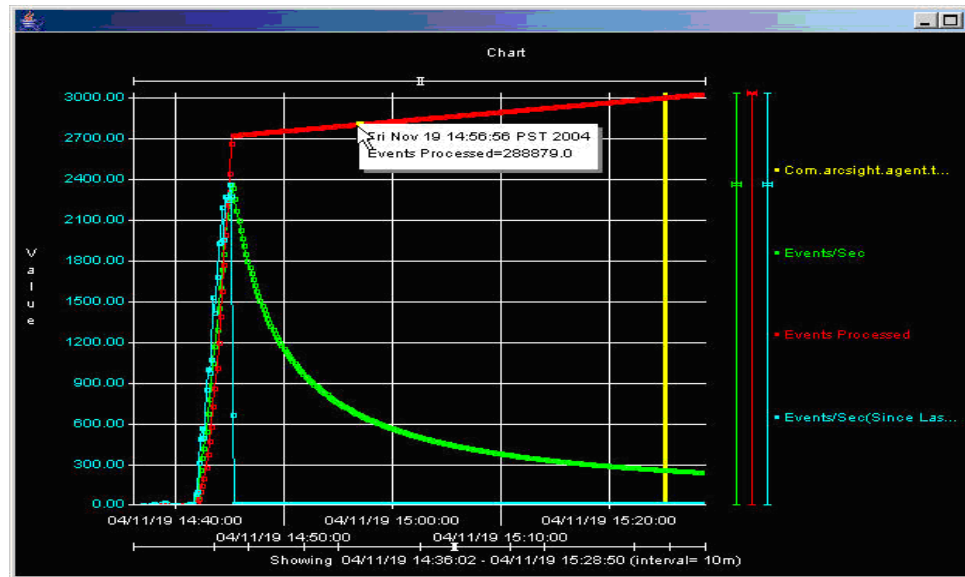
The initial display is always an empty grid. Loading very large log files can take a few minutes (a 100MB log might take 5 or 10 minutes). Once log files are scanned, the information gleaned from them is cached (in files named `data.*`), which speeds up loading the second time. If something about the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

Right-click the grid and choose **Show Plot/Event Window** from the context menu. Select what to show on the grid from the **Plot/Event Window** that appears.

The tree of possible things to display is divided into Plot—attributes that can be plotted over time, like events per second—and Event—one-time things, like exceptions, which are shown as vertical lines. Check as many things as you want to show.

Because SmartConnectors can talk to multiple Managers and each can be configured to use multiple threads for events, the Plot hierarchy includes nodes for each SmartConnector and each Manager. Within the SmartConnector, threads are named `E0`, `E1`, and so on. Each SmartConnector has one heartbeat thread (`H0`) as well. Different types of SmartConnector

(firewall log SmartConnector, IDS SNMP SmartConnector, and so on) have different attributes to be plotted.



The interactive Chart uses sliders to change the view. Hovering over a data point displays detailed information.

There are two horizontal sliders—one at the top of the grid, one underneath. The slider at the top indicates the time scale. Drag it to the right to zoom in, or widen the distance between time intervals (vertical lines). The slider at the bottom changes the interval between lines—anywhere from 1 second at the far left to 1 day at the far right. The time shown in the grid is listed below the bottom slider:

Showing YY/MM/DD HH:MM:SS - YY/MM/DD HH:MM:SS (Interval= X)

Click anywhere in the grid area and drag a green rectangle to zoom in, changing both the vertical and horizontal scales at once. Hold the **Ctrl** key as you drag to pan the window in the vertical or horizontal direction, and hold both the **Shift** and **Ctrl** keys as you drag to constrain the pan to either vertical or horizontal movement. When you are panning, only sampled data is shown, but when you stop moving, the complete data fills in. (You can change this by unchecking **Enable reduced data point rendering** in Preferences.)

Hover the mouse over a data point to see detailed information in a “tooltip” window, as shown in the figure, above..

For each attribute being plotted, a colored, vertical slider appears on the right of the grid. This slider adjusts the vertical (value) scale of the thing being plotted.

By default, data points are connected by lines. When data is missing, these lines can be misleading. To turn off lines, uncheck **Connect dots** in Preferences.

Once you have specified attributes of interest, scaled the values, centered and zoomed the display to show exactly the information of concern, select **Save as JPG** on the menu to create a snapshot of the grid display that you can print or e-mail. The size of the output image is the same as the grid window, so maximize the window to create a highly detailed snapshot, or reduce the window size to create a thumbnail.

Example

Perhaps a particular SmartConnector starts by sending 10 events per second (EPS) to the Manager, but soon is sending 100, then 500, then 1000 EPS before dropping back down to 10. Logfu lets you plot the SmartConnector's EPS over time—the result is something like a mountain peak.

When you plot the Manager's receipt of these events, you might see that it keeps up with the SmartConnector until 450 EPS or so. You notice that the Manager continues consuming 450 EPS even as the SmartConnector's EPS falls off. This is because the Manager is consuming events that were automatically cached.

By plotting the estimated cache size, you can see the whole story—the SmartConnector experienced a peak event volume and the cache stepped in to make sure that the Manager didn't lose events, even when it couldn't physically keep up with the SmartConnector.

Use the vertical sliders on the right to give each attribute a different scale to keep the peak EPS from the SmartConnector from obscuring the plot of the Manager's EPS.

Troubleshooting

Another real-world example involved a Check Point SmartConnector that was mysteriously down for almost seven days. Logfu plotted the event stream from the SmartConnector and it was clearly flat during the seven days, pinpointing the outage as well as the time that the event flow resumed. By overlaying Check Point Log Rotation events on the grid, it became clear that the event outage started with a Log Rotation and that event flow resumed coincident with a Log Rotation.

Further investigation revealed what had happened—the first Check Point Log Rotation failed due to lack of disk space, which shut down event flow from the device. When the disk space problem had been resolved, the customer completed the Log Rotation and event flow resumed.

If the Manager suddenly stops seeing events from a SmartConnector Logfu helps determine whether the SmartConnector is getting events from the device. Another common complaint is that not all events are getting through. Logfu has a plot attribute called 'ZFilter'—zone filter—that indicates how many raw device events are being filtered by the SmartConnector. Events processed (the number of events sent by the device) minus

ZFilter should equal Sent (the number of events sent to the Manager). A sample HTML report is shown below.

Logfu

Analizers

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

Sessions by Length

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

Sessions by Throughput

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

Sessions by Exception count

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

Sessions by longest Full GC

All Sessions

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

Session 0

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

Menu

Menu Item	Description
Show Plot/Event Window	Presents the possible attributes to be displayed
Bring To Front	
Send to Back	
Undo Zoom	Return to previous view
Zoom out	
Auto Scale	Fit all data on the grid
Save as JPG	Save a snapshot of the current view on the grid
Go to	Display the line of the log file which corresponds to a particular data point
Reset	Clear all checked attributes and restore the normal startup view of an empty grid
Preferences	Check: Connect dots – draw lines between data points Enable fast rendering Enable reduced data point rendering

Typical Data Attributes

SmartConnector Specific

Menu Item	Description
CommandResponses Processed	Number of Get Status calls from the Manager
Current Max Rate	
Events Processed	
Events/Sec	Averaged events per second
Events/Sec (Since Last Check)	Events per second in last minute (unless check time is configured to a different interval)
Max Rate	
contcachesize	Contiguous Cache Size
maxrate	Maximum Rate
maxsleeptime	Maximum Sleep Time
randomizeratetime	Randomize Rate Time
timefactor	

For Each SmartConnector Thread

Menu Item	Description
Average Batch Size	Number of events per batch (typically ~100)
Average Cycle Time	Duration of transport and Manager acknowledgement
Average Time Per Batch	Should be under 1 minute

Memory Usage

Menu Item	Description
Total	Total available memory
Used	Memory used

Events

Menu Item	Description
SmartConnectors Initializing	SmartConnector startup
com.arcsight.agent.transport. TransportException	
com.arcsight.common.agent. ServerConnectionException	
java.net.SocketException	
Forcing disconnection	Transport event—Manager disconnecting.

Intervals

1 second

5 seconds

10 seconds

30 seconds

1 minute

5 minutes

10 minutes

30 minutes

1 hour

6 hours

12 hours

1 day

Appendix E

Creating Custom E-mails Using Velocity Templates

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

This appendix is divided into the following sections:

[“Overview” on page 191](#)

[“Notification Velocity templates” on page 191](#)

A sample use case is presented to illustrate the concept.

Overview

ArcSight supports the use of Velocity templates that are a means of specifying dynamic input to the underlying Java code.

You can apply Velocity templates in a number of places in ArcSight. For a complete list of Velocity template applications in ArcSight, see the Console online Help.

This section describes one such application—E-mail Notification Messages—in detail. You can use Velocity templates on your Manager to create custom e-mail messages to suit your needs.

Notification Velocity templates

The `<ARCSIGHT_HOME>/Manager/config/notifications` directory contains the following two Velocity templates for customizing e-mail notifications:

- `Email.vm`—The primary template file that calls secondary template files.
- `Informative.vm`—The default secondary template file.

Commonly used elements in Email.vm and Informative.vm files

It is important to understand the commonly used Velocity programming elements in the `Email.vm` and `Informative.vm` files before editing these files.

The #if statement

The general format of the #if statement for string comparison is:

```
#if ($introspector.getDisplayValue($event, ArcSight_Meta_Tag)
Comparative_Operator Compared_Value)
```

The #if statement for integer comparison is:

```
#if ($introspector.getValue($event,
ArcSight_Meta_Tag).intValue() Comparative_Operator Compared_Value)
```

You can specify ArcSight_Meta_Tag, Comparative_Operator, and Compared_Value to suit your needs.

ArcSight_Meta_Tag is a string when using the #if statement for string comparison (for example, displayProduct) and is an integer for the #if statement for integer comparison (for example, severity).

For a complete listing of ArcSight meta tags, see the Token Mappings topic in ArcSight FlexConnector Guide.

Comparative_Operator is == for string comparison; =, >, and < for integer comparison.

Compared_Value is a string or an integer. For string comparison, enclose the value in double quotes (" ").

Contents of Email.vm and Informative.vm

The default Email.vm template file contents are:

```
## This is a velocity macro file...

## The following fields are defined in the velocity macro.

## event == the event which needs to be sent.

## EVENT_URL == root of the event alert.

## NOTIFICATION_URL == URL of the notifications page in ArcSight
Web

#parse ("Informative.vm")
```

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

- 1) Reply to this email. Make sure that the notification ID listed in this message is present in your reply)
- 2) Login to the ArcSight Console and click on the notification button on the status bar
- 3) Login to ArcSight Web at \${NOTIFICATION_URL}

To view the full alert please go to at \${EVENT_URL}

The default Informative.vm template file contents are:

```
=== Event Details ===
```



```
#foreach( $field in $introspector.fields )

#if( $introspector.getDisplayValue($event, $field).length() > 0 )

${field.fieldDisplayName}: $introspector.getDisplayValue($event,
$field)

#end

#end
```

Using Email.vm and Informative.vm Template Files

Email.vm calls the secondary template file Informative.vm (#parse ("Informative.vm")). The Informative.vm file lists all the non-empty fields of an event in the format `fieldName : fieldValue`.

Understanding the Customization Process

If you want to customize the template files to suit your needs, ArcSight recommends that you create new secondary templates containing fields that provide information you want to see in an e-mail for a specific condition.

For example, if you want to see complete details for an event—Threat Details, Source Details, Target Details, and any other information—generated by all Snort devices in your network, create a secondary template file called `Snort.vm` in `<ARCSIGHT_HOME>/config/notification`, on your Manager, with the following lines:

```
=== Complete Event Details ===
```

```
Threat Details
```

```
Event: $introspector.getDisplayValue($event, "name")
```

```
Description:
```

```
$introspector.getDisplayValue($event, "message")
```

```
Severity:
```

```
$introspector.getDisplayValue($event, "severity")
```

```
-----
```

```
Source Details
```

```
Source Address:
```

```
$introspector.getDisplayValue($event, "attackerAddress")
```

```
Source Host Name:
```

```
$introspector.getDisplayValue($event, "attackerHostName")
```

```
Source Port:
```

```
$introspector.getDisplayValue($event, "sourcePort")
```

```
Source User Name:
```

```
$introspector.getDisplayValue($event, "sourceUserName")
```

```
-----
```

```
Target Details
```

```
Target Address:
$introspector.getDisplayValue($event, "targetAddress")

Target Host Name:
$introspector.getDisplayValue($event, "targetHostName")

Target Port: $introspector.getDisplayValue($event, "targetPort")

Target User Name:
$introspector.getDisplayValue($event, "targetUserName")

-----

Extra Information (where applicable)

Transport Protocol:
$introspector.getDisplayValue($event, "transportProtocol")

Base Event Count:
$introspector.getDisplayValue($event, "baseEventCount")

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

-----
```

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

As shown in the example below, insert a condition to call `Snort.vm` if the `deviceProduct` in the generated event matches "Snort".

```
#if( $introspector.getDisplayValue($event, "deviceProduct") ==
"Snort" )

#parse("Snort.vm")

#else

#parse("Informative.vm")

#end
```

Customizing the template files

Follow these steps to customize the `Email.vm` and create any other secondary template files to receive customized e-mail notifications:

- 1 In `<ARCSIGHT_HOME>/config/notifications`, create a new secondary template file, as shown in the `Snort.vm` example in the previous section.
- 2 Save the file.
- 3 Edit `Email.vm` to insert the conditions, as shown in the example in the previous section.
- 4 Save `Email.vm`.

Sample Output

If you use the `Snort.vm` template and modify `Email.vm` as explained in the previous section, here is the output these templates generate:

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

=== Complete Event Details ===

Threat Details

Event:                      Internal to External Port Scanning

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

Severity:                   2

-----

Source Details

Source Address:             10.129.26.37

Source Host Name:

Source Port:                0

Source User Name:          jdoe

-----

Target Details

Target Address:             161.58.201.13

Target Host Name:

Target Port:                20090

Target User Name:

-----

Extra Information (where applicable)

Transport Protocol:        TCP

Base Event Count:          1

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

-----

How to Respond

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

1) Reply to this email. Make sure that the notification ID listed
in this message is present in your reply)

2) Login to the ArcSight Console and click on the notification
button on the status bar
```

3) Login to myArcSight and go to the My Notifications Acknowledgment page at
<https://mymanager.mycompany.com:9443/arcsight/app?service=page/NotifyHome>

View the full alert at

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

Configuration Changes Related to FIPS

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

[“Tools Used to Configure Components in FIPS” on page 198](#)
[“Types of Certificates Used in FIPS Mode” on page 199](#)
[“Some Often-Used SSL-Related Procedures” on page 207](#)
[“Setting up Server-Side Authentication” on page 212](#)
[“Setting up Client-Side Authentication” on page 212](#)
[“Changing the Password for NSS DB” on page 213](#)
[“Listing the Contents of the NSS DB” on page 214](#)
[“Viewing the Contents of a Certificate” on page 215](#)
[“Setting the Expiration Date of a Certificate” on page 215](#)
[“Deleting a Certificate from NSS DB” on page 215](#)
[“Replacing an Expired Certificate” on page 215](#)
[“Using the Certificate Revocation List \(CRL\)” on page 216](#)
[“Changing a Default Mode Installation to FIPS 140-2” on page 219](#)
[“Configure Your Browser for FIPS” on page 224](#)

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 the section [“Understanding SSL Authentication” on page 33](#).

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 [Appendix A, Administrative Commands, on page 115](#) 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 cypher 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 cypher suites are enabled for FIPS Suite B:

- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`

The Connector user password is used by a connector appliance to authenticate to the connector before being able to manage the connectors. If the default password is changed, then a SHA-256 hash of the password is saved on the connector's local file system for authenticating the connector user.

Passwords (and sometimes user names as well) for accessing event information in third party devices like databases, sensors, and so on, are obfuscated using 3DES encryption and saved on the connector's local file system.

Digests in HTTP posting of events to ESM as well as digests used in field obfuscation use SHA-256 in FIPS mode.

Event Integrity Algorithms use SHA-256, SHA-1, and SHA-512 in FIPS mode.

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

The “Installing ArcSight ESM in FIPS Mode” appendix in the ArcSight ESM Installation and Configuration Guide walks you through the steps to generate and use a self-signed certificate when doing a fresh installation in FIPS mode. 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.

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

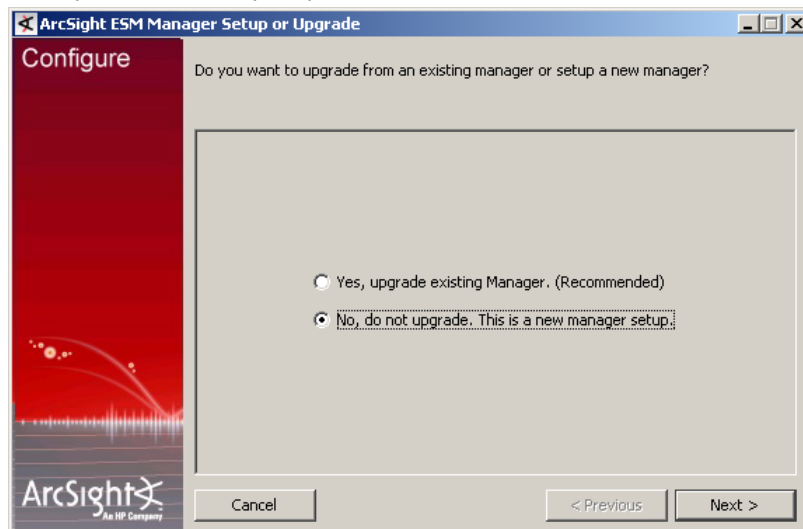
Below are the steps to configure your ArcSight server application to use a CA signed certificate in fips 140-2 mode.

- 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
<ARCSIGHT_HOME>/config/jetty/nssdb
```

- 4 Install the Manager by running its executable file.

- 5 When you get to the first configuration screen shown below, leave the wizard running and open a command prompt window.



- 1 Generate a key pair on the Manager by running the following from the Manager's /bin directory:
- 2 Generate a key pair on the Manager by running the following from the Manager's /bin directory:

For FIPS 140-2:

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

For Suite B:

```
./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
<ARCSIGHT_HOME>opt/arcsight/manager/config/jetty/nssdb
```

When prompted for a password, enter the default. The default is described in ["NSS database password" on page 37](#).

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

- 3 Verify key pair creation by entering the following command:

```
./arcsight runcertutil -K -d <absolute_path_to_Manager's_nssdb>
```

Enter the NSS DB password when prompted. The default is described in ["NSS database password" on page 37](#). You should see something similar to `<0> rsa <key>` in the output of the command.

- 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
<ARCSIGHT_HOME>/config/jetty/nssdb
```



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> .

To create a DER binary file:

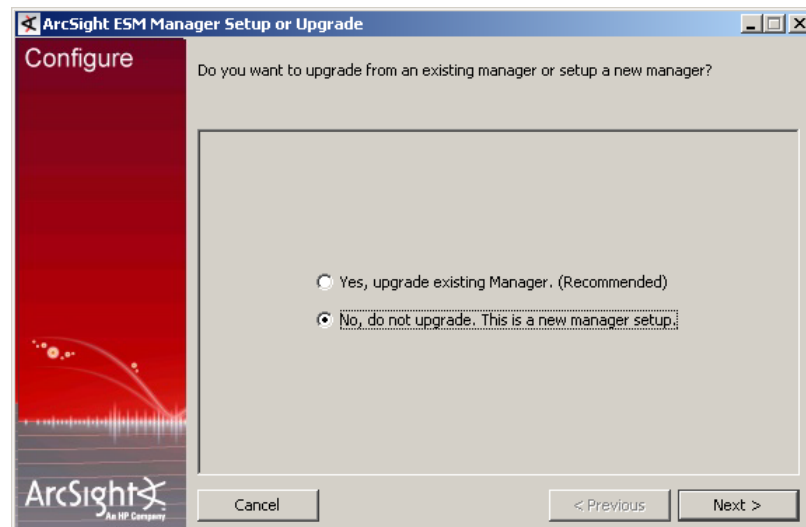
```
./arcsight runcertutil -R -s "CN=<hostname_or_IP>, O=<Name_of_organization>,
L=<City_where_the_organization_is_located>,
ST=<State_where_organization_is_located>, C=<Country>" -o
<absolute_path_to_filename.csr>
-d <ARCSIGHT_HOME>/config/jetty/nssdb
```

Enter the password for the NSS DB when prompted. The default is described in [“NSS database password” on page 37](#).

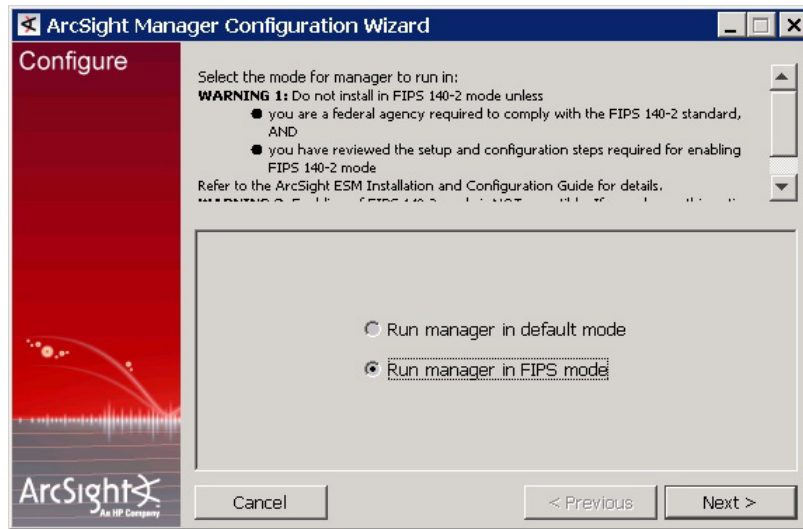
Enter random keyboard strokes when prompted to generate the random seed to generate your key.

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

- 5 Go back to the installation wizard screen and choose **No, do not upgrade. This is a new manager setup** to create a new, clean installation and click **Next**.

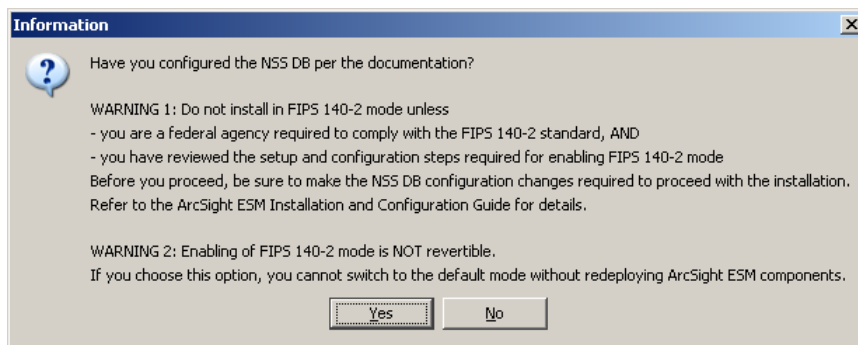


- 6 Next, you see the following screen:

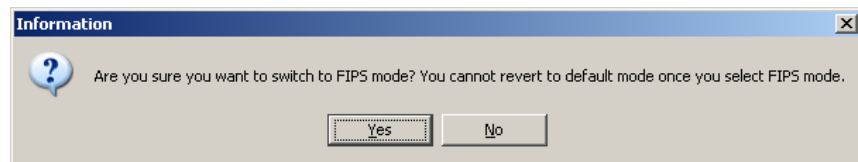


Select the **Run manager in FIPS mode** radio button and click **Next**.

- 7 The configuration wizard asks you to confirm that you have set up the NSS DB. Click **Yes**.



- 8 Acknowledge that once you select the FIPS mode, you cannot revert to the default mode. Click **Yes**.



- 9 Follow the prompts in the next few wizard screens to complete the Manager installation. Refer to "Installing ArcSight Manager" chapter in the ArcSight ESM Installation and Configuration Guide for details on any screen.
- 10 Send the `.csr` file to your Certificate Authority.
- The Certificate Authority sends you a key pair consisting of a private key and a public certificate signed by the CA.
- 11 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 <ARCSIGHT_HOME>/config/jetty/nssdb -i
<absolute_path_to_the_signed_certificate>
```

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

```
/sbin/service arcsight_services start manager
```

Steps Performed on ArcSight Web

ArcSight Web plays a dual role. On one hand, it acts as a client to the Manager to which it connects. On the other, it acts as a server to web browsers that connect to it. Therefore, ArcSight Web authenticates the Manager to which it connects and it also has to authenticate itself to web browsers.



Note

Make sure that you have copied the Manager's certificate to the machine on which you install ArcSight Web.

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
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

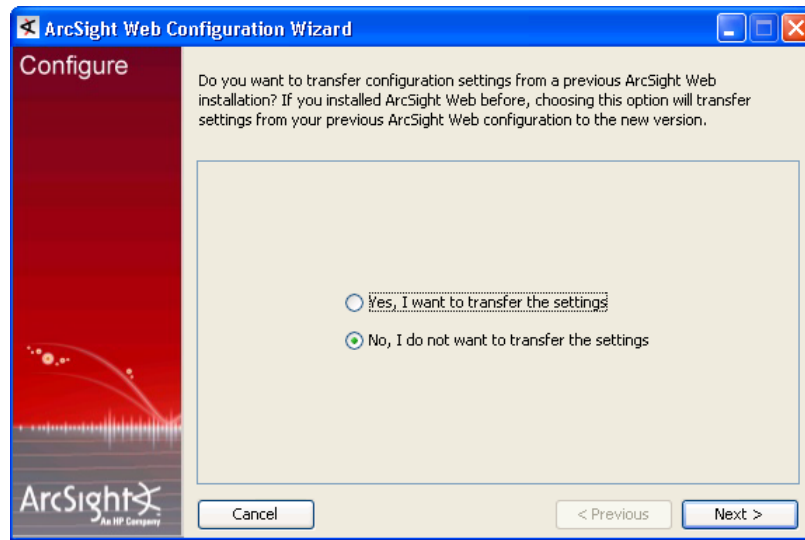
To authenticate the Manager, ArcSight Web's NSS DB should contain the CA's root certificate. At the same time, since the Web acts as a server to the web browsers that connect to it, you should have a key pair and a certificate containing ArcSight Web's public key in the Web's NSS DB. This allows ArcSight Web to authenticate itself to the web browsers.

You import the CA's root certificate into ArcSight Web's webnssdb. To obtain a CA-signed certificate for ArcSight Web, generate a key pair on ArcSight Web, generate a CSR on ArcSight Web, and send the CSR to the CA. Lastly, after you receive the signed certificate from the CA, import it into the webnssdb.

To accomplish all of the above:

1 Install ArcSight Web by running its executable file.

- When you get to the first configuration screen shown below, leave the wizard running and open a command prompt window.



- Import the CA's root certificate into the webnssdb by running the following from ArcSight Web's \bin directory. (For the -t option, make sure the you specify "CT,C,C" exactly as shown.)

```
./arcsight runcertutil -A -n <certificate_alias>
-t "CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_the_CA's_root_certificate>
```

This is required in order for ArcSight Web to be able to authenticate the Manager.

- Generate a key pair on ArcSight Web by running:

For FIPS 140-2:

```
./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 9258 -d
<ARCSIGHT_HOME>opt/arcsight/web/config/jetty/webnssdb
```

For Suite B:

```
./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
<ARCSIGHT_HOME>opt/arcsight/web/config/jetty/webnssdb
```

Enter the password for webnssdb when prompted. The default is described in ["NSS database password" on page 37](#).

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

- Verify that the key pair got created by entering the following command:

```
./arcsight runcertutil -K -d <absolute_path_to_Web's_webnssdb>
```

After entering the password, you should see something similar to <0> rsa <key> in the output of the command.

- 6 Generate a CSR in the webnssdb which you have to send to the CA to obtain a CA-signed certificate for ArcSight Web:

```
./arcsight runcertutil -R -s "CN=<previous_CN>,  
O=<company_name>, L=<Location_of_the_company>,  
ST=<State_where_company_is_located>, C=<country>" -a -o  
<absolute_path_to_the_filename.csr> -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb
```



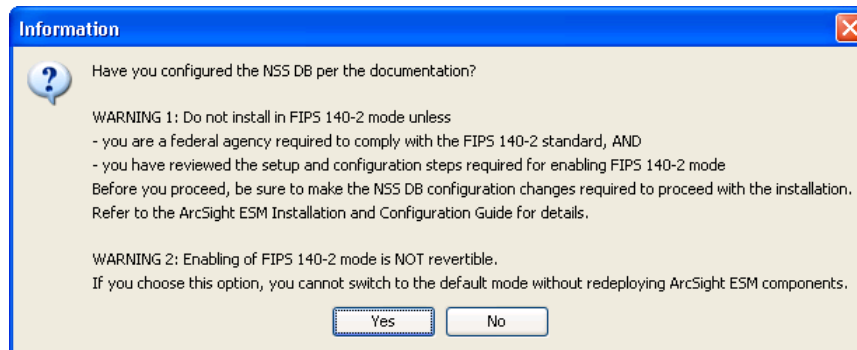
- Make sure the CN is either the IP address of the machine on which ArcSight Web resides or its fully qualified domain name used in the URL when you access ArcSight Web using a browser.
- If you do not specify the absolute path to where the .csr file should go, the path specified for the output file will be relative to <ARCSIGHT_HOME> .

This generates a CSR file that is placed in the location you had specified in the -o option in the command.

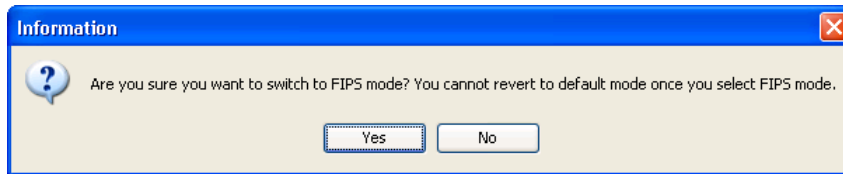
- 7 Go back to the wizard screen. Select **No, I do not want to transfer the settings** and click **Next**.
- 8 Select **Run web in FIPS mode** in the following screen and click **Next**:



- 9 The following prompt asks you whether you configured your webnssdb. Click **Yes**.

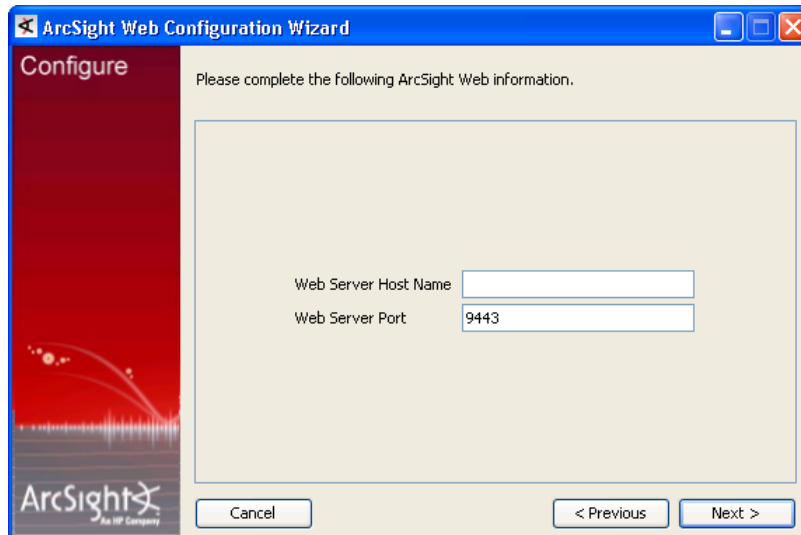


- 10 You see this warning message:



Click **Yes**.

- 11 When you get to the following screen, make sure that the Webserver Host name exactly matches the host name that you had entered for the webserver when installing the Manager. For example, if you had entered an IP address for the webserver in the Manager setup, make sure to enter the IP address in this screen too.



- 12 Follow the prompts in the next few wizard screens and complete the wizard.

- 13 Send the .csr file to your Certificate Authority.

The Certificate Authority sends you a key pair consisting of a private key and a public certificate signed by the CA.

- 14 After you receive ArcSight Web's signed certificate from the CA, import it into ArcSight Web's webnssdb by running:

```
./arcsight runcertutil -A -n mykey
-t "C,C,C" -d <ARCSIGHT_HOME>web/config/jetty/webnssdb -i
<absolute_path_to_ArcSight_Web_certificate>
```

The web browsers that connect to the webserver use ArcSight Web's certificate to authenticate the webserver.

- 15 Start ArcSight Web by running the following from its /bin directory as user *arcsight*:

```
/sbin/service arcsight_services start arcsight_web
```

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.



Make sure that you have copied the CA root certificate to the machine on which 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



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

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

On the Manager

- 1 Run the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory to generate a key pair:

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

**Note**

- 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. Using *-v* is optional. If you choose to use it, see [“Setting the Expiration Date of a Certificate” on page 215](#) for details. To see the validity period of an existing certificate, see [“Viewing Certificate Details” on page 43](#).

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
<ARCSIGHT_HOME>/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 37](#).
- 3 Enter random keyboard strokes when prompted, to generate the random seed used to generate your key.

On ArcSight Web

To create a key pair on the Web server:

- 1 Run the following command from ArcSight Web's */bin* directory:

```
./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey -k
rsa -x -t "C,C,C" -m 2345 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

- ◆ The *-m* serial number (2345) must be unique within *webnssdb*. That is, it must be different than the one for the Manager's key pair.
 - ◆ *hostname* is the name of the machine on which ArcSight Web is installed.
 - ◆ Using *-v* is optional. If you choose to use it, see [“Setting the Expiration Date of a Certificate” on page 215](#) for details.
- 2 Enter the password for *webnssdb*. The default is described in [“NSS database password” on page 37](#).
 - 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>
```



When you import or generate a key pair into NSS DB, if there is a 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, you need to 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 in order to import it into the client that wishes to connect to the server.

Likewise, for client side authentication, you need to have the client's certificate in the NSS DB of both the client and the server. Export the client's certificate from the client's NSS DB in order 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 <ARCSIGHT_HOME>/config/jetty/nssdb -o <absolute_path_to_where_you_want_certificate_exported>
```

For example:

```
./arcsight runcertutil -L -n mykey -r -d <ARCSIGHT_HOME>/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`.



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>
```



If you do not specify the absolute path for the .cer file, it gets placed in the Console's [<ARCSIGHT_HOME>](#) folder.

Exporting a Certificate From the Web

To export the Web's certificate, run the following from the Web's /bin directory:

```
./arcsight runcertutil -L -n <alias_for_exported_certificate> -r -d  
<ARCSIGHT_HOME>/config/jetty/webnssdb -o  
<full_path_to_where_you_want_certificate_exported>
```



If you do not specify the absolute path for the .cer file, it gets placed in the Web's [<ARCSIGHT_HOME>](#) 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, the server's certificate needs to be imported into the client's NSS DB. For client side authentication, the client's certificate needs to be imported into the server's NSS DB.

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 <ARCSIGHT_HOME>/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.

On ArcSight Web

To import the Manager's certificate into ArcSight Web's webnssdb:

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

For the `-t` option, be sure to use CT,C,C 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 key pair being imported has an alias that matches a pre-existing key pair, the key pair fails to import citing an error:

```
PKCS12 decode validate bags failed: The user pressed cancel.
```

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

On the Manager:

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

On the Web:

```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

On the Console:

```
arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
<ARCSIGHT_HOME>\current\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 Manager:

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

On Web:

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

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

Setting up Server-Side Authentication

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

The ArcSight ESM Installation and Configuration Guide walks you through the steps for installing ESM with server-side authentication.

Setting up Client-Side Authentication

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

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

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

- 1 Stop the Console if it is running.
- 2 Generate a key pair in the Console's `nssdb.client`. Follow the steps in [“Generating a Key Pair in a Component's NSS DB” on page 207](#) (“On the Console” subsection). This automatically generates a self-signed certificate on the Console's NSS DB.

Alternatively, you can use an existing key pair which you have to import into the Console's NSS DB. See [“Importing an Existing Key Pair into the NSS DB” on page 211](#) for details.

- 3 Export the Console's certificate. See the section [“Exporting Certificates” on page 209](#) (“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 210](#) (“On the Manager” subsection) for details.



Caution

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

- 6 Restart the Manager, then Console.

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

- 1 Stop the Console if it is running.
- 2 Generate a key pair on the Console. See the [“Generating a Key Pair in a Component's NSS DB” on page 207](#) for details.

- 3 Generate a CSR on the Console by running the following from the Console's \bin directory:

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



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

- 4 Send the CSR file to your CA and obtain a signed certificate from your CA.
- 5 Import the CA-signed certificate into the Console's nssdb.client. See ["Importing a Certificate into the NSS DB" on page 210](#) (subsection "On the Console") for details.
- 6 Stop the Manager if it is running.
- 7 Import the Console's CA-signed certificate into the Manager's nssdb. See ["Importing a Certificate into the NSS DB" on page 210](#) (subsection "On the Manager") for details.

Changing the Password for NSS DB

ESM ships with a default password for the NSS DB (see ["NSS database password" on page 37](#)). ArcSight recommends that you change the password on each component before moving to a production environment. To do so:

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

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

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

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

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

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

- 4 Enter the old password and a new password and confirm it when prompted.
- 5 Re-enable FIPS mode on the NSS DB:

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

- 6 Open the properties file:

On the Manager:

Located in: <ARCSIGHT_HOME>/config/server.properties.

Change

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

to

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

On the Console:

Located in <ARCSIGHT_HOME>\current\config\console.properties

Change

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

to

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

On the Web:

Located in <ARCSIGHT_HOME>/config/webserver.properties.

Change

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

to

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

7 Run the setup program from the component's /bin directory:

Manager:

```
./arcsight managersetup
```

Console:

```
arcsight consolesetup
```

Web:

```
./arcsight webserversetup
```

and accept all the defaults in the wizard. This is required in order to obfuscate the password that you had entered in plain text.

Listing the Contents of the NSS DB

After you import a certificate or generate a key pair in a component's NSS DB, you can verify that the certificate import was successful or the key pair has been successfully generated. You can do this by listing the contents of the NSS DB. To view the contents of a component's NSS DB, run the following command from the component's /bin directory:

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

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

Viewing the Contents of a Certificate

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

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

Setting the Expiration Date of a Certificate

To set the expiry date of the certificate, you have to do so when generating the key pair. Once you have generated the key pair, you cannot change the expiration date on the certificate and the certificate 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 [Appendix A, Administrative Commands](#), on page 115 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 a server (Manager or Web), you need to replace it with a new one. You can see when a certificate will expire by opening it.

To replace the certificate:

- 1 Stop the server if it is running.
- 2 Delete the expired certificate from the server's NSS DB. See ["Deleting a Certificate from NSS DB" on page 215](#) for details.

Since the common name (CN) for the new certificate is identical to the CN in the old certificate, you are not permitted to have both the expired as well as the new certificate co-exist in the NSS DB.
- 3 In case of CA-signed certificate, replace the certificate by importing the new certificate into the server's NSS DB.

In case of self-signed certificate, you have to generate a key pair on the server. See [“Generating a Key Pair in a Component’s NSS DB” on page 207](#) for details on how to do this. Generating the key pair automatically generates the certificate.

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

For example, if your Manager’s certificate has expired, you have to

- a** Delete the expired certificate from the Manager’s `nssdb`. See [“Deleting a Certificate from NSS DB” on page 215](#)
- 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 207](#)
- c** Export the newly generated certificate from the Manager. See [“Exporting Certificates” on page 209](#)
- d** Delete the expired Manager’s certificate from the Console’s and Web’s NSS DB.
- e** Generate a new keypair in the Web’s `nssdb` which effectively generates a new certificate on the Web. See [“Generating a Key Pair in a Component’s NSS DB” on page 207](#)
- f** Import the Manager’s new certificate into the Console’s and Web’s NSS DB. See [“Importing a Certificate into the NSS DB” on page 210](#)

Using the Certificate Revocation List (CRL)

Starting in v4.0 SP2, 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 `<ARCSIGHT_HOME>/config/jetty/nssdb` directory

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

- You have a current CRL file provided by your CA.
The CA updates the CRL file periodically as and when additional certificates get invalidated.

To use the CRL feature:

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

After adding the CRL file, it takes 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 Keypair 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 a 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.

- a** 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, you have to do so when generating the key pair. Once you have generated the key pair, you cannot change the expiry date on the certificate.



Caution

- Make sure to use "mykey" (without quotes) as the alias name for the key pair as shown in the example.
- The `-m` serial number should be unique within `nssdb`
- The hostname is the short name or fully qualified domain name depending upon how your 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 215](#) 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  
<ARCSIGHT_HOME>/config/jetty/nssdb
```

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  
<ARCSIGHT_HOME>/config/jetty/nssdb
```

Entered the password, when prompted. The default is described in ["NSS database password" on page 37](#).

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`.

- b** 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 `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d  
<ARCSIGHT_HOME>/config/jetty/nssdb -o <absolute_path_to  
_managercertificatename.cert>
```



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 `<ARCSIGHT_HOME>` directory by default.

For example, to export the certificate as a file named `ManagerCert.cer` to `C:\arcsight\Manager` directory, run:

```
./arcsight runcertutil -L -n mykey -r -d  
<ARCSIGHT_HOME>/config/jetty/nssdb -o  
<ARCSIGHT_HOME>/ManagerCert.cer
```

This generates the `ManagerCert.cer` file, the Manager's certificate, in the `/<ARCSIGHT_HOME>` directory.

Importing a Certificate into the Manager

Import a certificate into the Manager:

```
./arcsight runcertutil -A -n <certificate_name> -t "CT,C,C" -d  
<ARCSIGHT_HOME>/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, you have to 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

To convert an existing Manager from default mode to FIPS mode:

- 1 Log in as user 'arcsight'.
- 2 Stop the Manager if it is running. In the command prompt window for the running manager, click CTR-C to initiate shutdown. When it asks "Terminate batch job (Y/N)?" click Y.
- 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 `<ARCSIGHT_HOME>/config/jetty/keystore`.
 - c When prompted, enter the password that you set for the keystore. For the default, see ["Keystore password" on page 37](#).
 - 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 Export the Manager's certificate from the Manager's truststore located in the Manager's `/jre/lib/security/cacerts` using the keytoolgui.
 - a Start the keytoolgui by running the following from the Manager's `/bin` directory if it is not already running:
`./arcsight keytoolgui`

- b** Click **File->Open KeyStore** and navigate to the Manager's `/jre/lib/security/cacerts`.
- c** Enter a password that you had set for the keystore when prompted. For the default, see ["Keystore password" on page 37](#).
- d** Right-click the Manager's certificate and select **Export**. If the Manager uses a CA-signed certificate, export the CA's root certificate instead.
- e** Click **OK** in the Export Keystore dialog.
- f** Navigate to the location on your machine to where you want to export the certificate.
- g** Enter a name for the certificate with a `.cer` extension in the Filename textbox and click **Export**.
- h** You will see an `Export Successful` message. Click **OK**.
- i** Exit the `keytoolgui`.

Press **Enter** on your keyboard when prompted.

- 5** Import the Manager's key pair that you had exported in [Step 3 on page 219](#) 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  
/config/jetty/nssdb
```

Enter the password for the Manager's `nssdb` when prompted. The default is described in ["NSS database password" on page 37](#).

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.

- 6** 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 /config/jetty/nssdb
```

- 7** Run the Manager setup program from the Manager's `/bin` directory:

```
./arcsight managersetup
```

- 8** Import the Manager's certificate that you had exported in [Step 4 on page 219](#) into the Manager's `/config/jetty/nssdb`. Run the following command from the Manager's `bin` directory to import the certificate into the Manager's `nssdb`:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t  
"CT,C,C" -d /config/jetty/nssdb -i  
<absolute_path_to_manager's_certificate>
```



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

- 9** Select **Run Manager in FIPS mode**.
- 10** Follow the prompts in the next few screens until the wizard informs you that you have successfully configured the Manager. Refer to the chapter, ["Installing ArcSight Manager" on page 83](#) if you need more information on any wizard screen.

- 11 Restart the Manager.
- 12 If you had upgraded your Manager from v4.0 SP1 or earlier version, you will also be required to reset all user passwords by running the following command from the Manager's /bin directory:

```
./arcsight batchresetpwd -f <absolute_path_to_password_file>
```

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`.

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 <ARCSIGHT_HOME>/bin directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d  
<ARCSIGHT_HOME>/config/jetty/nssdb -o <absolute_path_to  
_managercertificatename.cert>
```



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 37](#).
 - 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**.
- 5 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
```
- 6 Run the Console's setup program by running the following from the Console's `\bin` directory:
- ```
arcsight consolesetup
```
- 7 Select **No, I do not want to transfer the settings**.
- 8 Select **Run Console in FIPS mode**.
- 9 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**.
- 10 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.
- 11 Set your browser to use FIPS. See ["Configure Your Browser for FIPS" on page 224](#).

ArcSight Web

To convert an existing ArcSight Web running in default mode to run in FIPS mode, you have to migrate ArcSight Web's key pair, certificate, and the Manager's certificate from ArcSight Web's keystore and truststore into its `webnssdb` as described in the procedure below. ArcSight Web's certificates and key pairs are stored in the `webkeystore` while the Manager's certificates are stored in ArcSight Web's `cacerts`.

- 1 Stop ArcSight Web if it is running. Use this command run as user *arcsight*:
- ```
/sbin/service arcsight_services stop arcsight_web
```
- 2 Export ArcSight Web's key pair from `<ARCSIGHT_HOME>/config/jetty/webkeystore` to a location of your choice. Make sure that you name it `mykey.pfx`.
- a Start the keytoolgui by running the following from ArcSight Web's `//bin` directory:

```
./arcsight keytoolgui
```

- b** Click **File->Open KeyStore** and navigate to ArcSight Web's `//config/jetty/webkeystore`.
  - c** When prompted, enter the password that you set for the keystore. For the default password, see ["Keystore password" on page 37](#).
  - 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** 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**.
- 3** Export the Manager's certificate from the Manager's truststore located in the Manager's `<ARCSIGHT_HOME>manager/jre/lib/security/cacerts` using the `keytoolgui`.
  - a** Start the `keytoolgui` by running the following from the Manager's `/bin` directory if it is not already running:
 

```
./arcsight keytoolgui
```
  - b** Click **File->Open KeyStore** and navigate to the Manager's `/jre/lib/security/cacerts`.
  - c** Enter a password that you had set for the keystore when prompted. For the default password, see ["Keystore password" on page 37](#).
  - d** Right-click the Manager's certificate and select **Export**. If the Manager uses a CA-signed certificate, export the CA's root certificate instead.
  - e** Click **OK** in the Export Keystore dialog.
  - f** Navigate to the location on your machine to where you want to export the certificate.
  - g** Enter a name for the certificate with a `.cer` extension in the Filename textbox and click **Export**.
  - h** An `Export Successful` message appears. Click **OK**.
  - i** Exit the `keytoolgui`.
- 4** Import ArcSight Web's key pair which you exported in [Step 2](#) into its `<ARCSIGHT_HOME>/config/jetty/webnssdb` by running the following command from its `/bin` directory:
 

```
./arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```
- 5** Run the following command from your ArcSight Web's `<ARCSIGHT_HOME>/bin` directory to verify that the key pair is imported correctly. Note that the alias of the key pair that you just imported in the `webnssdb` is the same as the alias of that key pair in the `.pfx` file.
 

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

This command lists the contents of the webnssdb. Make sure that mykey is listed in the output.

- 6 Import the Manager's certificate which you exported in Step 3a into its /config/jetty/webnssdb by running the following command from its /bin directory:

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_manager's_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.

---

- 7 Run ArcSight Web's setup program by running the following from ArcSight Web's \bin directory:

```
./arcsight webserversetup
```

- 8 Select **Run web in FIPS mode**.
- 9 Follow the prompts in the next few screens until the wizard informs you that you have successfully configured ArcSight Web.
- 10 restart ArcSight Web by running this command:  

```
/sbin/service arcsight_services start arcsight_web
```
- 11 Set your browser to use FIPS, as described in the following topic.

## 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 ArcSight Web.

### FIPS with Firefox

FIPS can be configured for versions of Firefox up to version 14. The steps for Firefox are more involved than for other browsers, so they are included here.

- 1 In the Firefox window, select **Tools->Options...** (or **Edit->Preferences** in the case of Firefox on Linux)
- 2 In the Options window, click the **Advanced** icon.
- 3 Click the **Encryptions** tab to open the page.
- 4 Uncheck the **Use SSL 3.0** check box.
- 5 Check the **Use TLS 1.0** check box.
- 6 Click the **Security Devices** button to open the Device Manager dialog where you will enable FIPS in Firefox's NSS internal PKCS #11 module.
- 7 Click **Software Security Device** and click **Change Password** button.
- 8 Enter a new password and re-enter it to confirm it.



- 9 Select **NSS Internal PKCS #11 Module** and click **Enable FIPS** button.
- 10 Click **OK** to close the Device Manager window and click **OK** to close the Preferences window.
- 11 You must disable all non-FIPS TLS cipher suites. In the location box of the Firefox browser, enter `about:config` and press **Enter**.
- 12 In the message that follows, click the **I'll be careful, I promise** button.
- 13 In the **Filter** textbox, type `ssl`.
- 14 Compare the true/false value for each preference listed on the page that follows with the preference Value in the screenshot below and make sure that the true/false value

match the ones shown in the screenshot below. If any preference value does not match, double click its value to toggle it.

| Preference Name                               | Status          | Type           | Value        |
|-----------------------------------------------|-----------------|----------------|--------------|
| security.enable_ssl2                          | default         | boolean        | false        |
| <b>security.enable_ssl3</b>                   | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl2.des_64                          | default         | boolean        | false        |
| security.ssl2.des_ede3_192                    | default         | boolean        | false        |
| security.ssl2.rc2_128                         | default         | boolean        | false        |
| security.ssl2.rc2_40                          | default         | boolean        | false        |
| security.ssl2.rc4_128                         | default         | boolean        | false        |
| security.ssl2.rc4_40                          | default         | boolean        | false        |
| security.ssl3.dhe_dss_aes_128_sha             | default         | boolean        | true         |
| security.ssl3.dhe_dss_aes_256_sha             | default         | boolean        | true         |
| <b>security.ssl3.dhe_dss_camellia_128_sha</b> | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| <b>security.ssl3.dhe_dss_camellia_256_sha</b> | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.dhe_dss_des_ede3_sha            | default         | boolean        | true         |
| security.ssl3.dhe_dss_des_sha                 | default         | boolean        | false        |
| security.ssl3.dhe_rsa_aes_128_sha             | default         | boolean        | true         |
| security.ssl3.dhe_rsa_aes_256_sha             | default         | boolean        | true         |
| <b>security.ssl3.dhe_rsa_camellia_128_sha</b> | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| <b>security.ssl3.dhe_rsa_camellia_256_sha</b> | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.dhe_rsa_des_ede3_sha            | default         | boolean        | true         |
| security.ssl3.dhe_rsa_des_sha                 | default         | boolean        | false        |
| security.ssl3.ecdh_ecdsa_aes_128_sha          | default         | boolean        | true         |
| security.ssl3.ecdh_ecdsa_aes_256_sha          | default         | boolean        | true         |
| security.ssl3.ecdh_ecdsa_des_ede3_sha         | default         | boolean        | true         |
| security.ssl3.ecdh_ecdsa_null_sha             | default         | boolean        | false        |
| <b>security.ssl3.ecdh_ecdsa_rc4_128_sha</b>   | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.ecdh_rsa_aes_128_sha            | default         | boolean        | true         |
| security.ssl3.ecdh_rsa_aes_256_sha            | default         | boolean        | true         |
| security.ssl3.ecdh_rsa_des_ede3_sha           | default         | boolean        | true         |
| security.ssl3.ecdh_rsa_null_sha               | default         | boolean        | false        |
| <b>security.ssl3.ecdh_rsa_rc4_128_sha</b>     | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.ecdhe_ecdsa_aes_128_sha         | default         | boolean        | true         |
| security.ssl3.ecdhe_ecdsa_aes_256_sha         | default         | boolean        | true         |
| security.ssl3.ecdhe_ecdsa_des_ede3_sha        | default         | boolean        | true         |
| security.ssl3.ecdhe_ecdsa_null_sha            | default         | boolean        | false        |
| <b>security.ssl3.ecdhe_ecdsa_rc4_128_sha</b>  | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.ecdhe_rsa_aes_128_sha           | default         | boolean        | true         |
| security.ssl3.ecdhe_rsa_aes_256_sha           | default         | boolean        | true         |
| security.ssl3.ecdhe_rsa_des_ede3_sha          | default         | boolean        | true         |
| security.ssl3.ecdhe_rsa_null_sha              | default         | boolean        | false        |
| <b>security.ssl3.ecdhe_rsa_rc4_128_sha</b>    | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.rsa_1024_des_cbc_sha            | default         | boolean        | false        |
| security.ssl3.rsa_1024_rc4_56_sha             | default         | boolean        | false        |
| security.ssl3.rsa_aes_128_sha                 | default         | boolean        | true         |
| security.ssl3.rsa_aes_256_sha                 | default         | boolean        | true         |
| <b>security.ssl3.rsa_camellia_128_sha</b>     | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| <b>security.ssl3.rsa_camellia_256_sha</b>     | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.rsa_des_ede3_sha                | default         | boolean        | true         |
| security.ssl3.rsa_des_sha                     | default         | boolean        | false        |
| <b>security.ssl3.rsa_fips_des_ede3_sha</b>    | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.rsa_fips_des_sha                | default         | boolean        | false        |
| security.ssl3.rsa_null_md5                    | default         | boolean        | false        |
| security.ssl3.rsa_null_sha                    | default         | boolean        | false        |
| security.ssl3.rsa_rc2_40_md5                  | default         | boolean        | false        |
| <b>security.ssl3.rsa_rc4_128_md5</b>          | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| <b>security.ssl3.rsa_rc4_128_sha</b>          | <b>user set</b> | <b>boolean</b> | <b>false</b> |
| security.ssl3.rsa_rc4_40_md5                  | default         | boolean        | false        |

**15** In addition, change the preference `network.http.spdy.enabled` to `false`.

**16** Disable the TLS Ticket Extension as follows:

- a** In the Filter textbox, enter TLS.
- b** Change the value of `security.enable_tls_session_tickets` preference to `false` by double-clicking it.

- c** Quit the browser and restart it; then connect to the webserver.

## Partition Archiver

To convert an existing Partition Archiver running in default mode to run in FIPS mode, you must import the Manager's certificate and in case the Manager uses a CA-signed certificate, the root certificate of the CA into the Partition Archiver's `nssdb.client`. To do so:

- 1** Export the Manager's certificate by running the following command from the Manager's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d
/config/jetty/nssdb -o <absolute_path_to
_Manager's_certificate>
```

In case, the Manager uses a CA-signed certificate, make sure to export the CA's root certificate from the Manager.

- 2** Import Manager's certificate (and the CA's root certificate in case of CA-signed certificate) into the Database's `usr/agent/nssdb.client` by running the following command from the Database's `bin` directory:

```
./arcsight runcertutil -A -n <manager_certificate_alias> -t
"CT,C,C" -d /usr/agent/nssdb.client -i
<absolute_path_to_the_manager's_certificate>
```

- 3** Run this command from the Database's `bin` directory:

```
./arcsight agentsetup
```

and follow the prompts on the screen to set up Partition Archiver in FIPS mode. Be sure to select the FIPS mode option when prompted for the mode in which to install.



## Symbols

#if statement 192

## A

- access control list (ACL) 102
- ACLReportGen command 116
- Active Directory, setting up authentication for 102
- actors
  - configuring 90
- agent logfu command 116
- agent tempca command 117
- agentcommand command 117
- agentsvc command 118
- agenttempca command 118
- agentup command 118
- anti-virus scan impact 13
- arcdbutil command 118
- arcdt command 119
- archive
  - task syntax 125
- archive command 120
- archivefilter command 126
- archivewizard command 127
- ArcSight Console
  - adjust memory 23
  - FIPS setup 207
  - session timeout 76
- ArcSight Express Appliance
  - configuring 95
- ArcSight Web
  - session timeout 76
- authentication 101
  - Active Directory 102
  - built-in 102
  - client-side 212
  - custom JAAS plug-in configuration 104
  - external 101
  - LDAP 104
  - password-based 102
  - PKCS#11 101
  - RADIUS 102
  - server-side 212
  - SSL client-only 105
  - using certificates 74

## B

- bleep command 128
- bleepsetup command 128
- built-in authentication 102

## C

- CA-signed certificate 46, 51
  - import 53
  - obtaining 52
- certificate
  - certificate authority 199
  - expiration 215
  - export 209
  - import 210
  - in FIPS 199
  - migrating type-to-type 72
  - revocation list (CRL) 216
  - self-signed vs. CA-signed 46
  - signing request 199
  - view contents 209, 215
- changepassword command 129
- character set in passwords 77
- checklist command 129
- Cipher suite
  - default mode 37
- cipher suites 37
- client keystore 105
- command help 198
- commands
  - ACLReportGen 116
  - agent logfu 116
  - agent tempca 117
  - agentcommand 117
  - agentsvc 118
  - agenttempca 118
  - agentup 118
  - arcdbutil 118
  - arcdt 119
  - archive 120
  - archivefilter 126
  - archivewizard 127
  - bleep 128
  - bleepsetup 128
  - changepassword 129
  - checklist 129
  - console 129
  - consolesetup 130
  - database pc 130
  - database pm 131
  - database xts 132
  - databasesetup 132
  - dbcheck 132
  - dbview-generator 133
  - deploylicense 133
  - downloadcertificate 133
  - drops|partitions 134

- exceptions 134
- export\_system\_tables 135
- flexagentwizard 136
- groupconflictingassets 136
- idefensesetup 137
- import\_system\_tables 137
- keytool 138
- keytoolgui 138
- kickbleep 138
- listsubjectdns 139
- logfu 139
- manager 140
- managerinventory 140
- manager-no-wrapper 140
- manager-reload-config 141
- managersetup 141
- managerstop 142
- managersvc 142
- managerthreaddump 142
- managerup 142
- monitor 143
- netio 143
- package 144
- portinfo 145
- querytuner 146
- reenableuser 147
- refcheck 148
- regex 148
- replayfilegen 148
- resetpwd 149
- resvalidate 149
- ruledesc 150
- runcertutil 150
- runmodeutil 152
- runpk12util 152
- script 153
- searchindex 153
- sendlogs 154
- tee 154
- tempca 154
- testbedconnection 155
- threaddumps 155
- tproc 156
- uninstallservice 156
- webserver 157
- webserver-no-wrapper 157
- webserversetup 157
- webserversvc 157
- websetup 158
- whois 158
- compression mode 84
- configuration
  - ArcSight Web as a service 11
  - database monitor 86
  - database monitor e-mail recipients 86
  - Manager as a service 11
  - Manager logging 24
  - Oracle free-space check 87
  - SNMP trap sender 87
- configuring
  - SSL 103
- console command 129
- consolesetup command 130
- custom authentication scheme 104

- cypher suite
  - FIPS 198

## D

- data
  - export 110
- database
  - backup 109
  - check task
    - disable 178
    - list 179
  - checks 177
  - pc command 130
  - pm command 131
  - recovery 110
  - set threshold notification 108
  - xts command 132
- databasesetup command 132
- dbcheck command 132
- dbview-generator command 133
- deploylicense command 133
- diagnostic information 26
- digests 198
- downloadcertificate command 133
- dropSLPartitions command 134
- dynamic properties 19

## E

- Email.vm file
  - contents 192
  - elements 191
  - how it works 193
- encryption 37
  - FIPS 198
- events
  - integrity algorithms 198
  - send as SNMP trap 87
- exceptions command 134
- expiration, certificate 215
- export\_system\_tables command 135
- external authentication 101
  - guidelines 101

## F

- failed logins, restricting 79
- FIPS 140-2 197
- flexagentwizard command 136
- free space monitoring 108

## G

- groupconflictingassets command 136

## I

- idefensesetup command 137
- import\_system\_tables command 137
- Informative.vm file
  - contents 192
  - elements 191
  - how it works 193
- initialization parameters, Oracle, changing 107

**J**

JAAS plug-in authentication 104

**K**

key pair, importing 211  
keytool command 138  
    detailed usage 43  
keytoolgui command 138  
    in SSL configuration 38  
kickbleep command 138

**L**

LDAP  
    setting up authentication for 104  
license  
    file import 24  
listsubjectdns command 139  
logfu  
    command 139  
    data attributes 188  
    Example 186  
    example 124  
    intervals 189  
    menu 188  
login  
    custom message 14  
    restricting failures 79  
logs  
    gathering 26

**M**

Manager  
    change ports 75  
    change properties dynamically 21  
    decoupled process execution 10  
    FIPS setup 199  
    Password Configuration 76  
    reconfigure 75  
    reconnect 10  
    remove service on Windows 12  
manager command 140  
managerinventory command 140  
manager-no-wrapper command 140  
manager-reload-config command 141  
managersetup command 141  
managerstop command 142  
managersvc command 142  
managethreaddump command 142  
managerup command 142  
memory, adjust 23  
monitor command 143

**N**

netio command 143  
Network Security Services (NSS) 198  
notification velocity templates 191

**O**

Oracle  
    password reset 109

**P**

package command 144  
partitions  
    compression speed 110  
    logs 111  
password-based authentication 102  
passwords  
    and character sets 77  
    check with regular expressions 78  
    guidelines 76  
    obfuscation 198  
    set expiration 79  
PKCS#11 authentication 101  
port, Manager, changing 75  
portinfo  
    command 145  
properties file  
    change dynamically for Manager 21  
    editing 18  
    format 17  
    secure 22

**Q**

querytuner command 146

**R**

RADIUS  
    setting up authentication for 102  
reenableuser command 147  
refcheck command 148  
regex command 148  
replayfilegen command 148  
resetpwd command 149  
resources  
    import from archive 125  
resvalidate command 149  
revocation list, certificate 216  
ruledesc command 150  
runcertutil 198  
runcertutil command 150  
runmodutil command 152  
runpk12util command 152

**S**

script command 153  
searchindex command 153  
self-signed certificate 46  
send logs  
    utility 26  
sendlogs  
    command 154  
SmartConnectors  
    event compression 84  
    start 11  
SNMP trap, send events as 87  
SSL  
    client-only authentication 105  
    configuring 103, 104  
SSL authentication  
    CA-signed certificate 51  
    certificate 45  
    configuration tools 38

- how it works 44
- overview 33
- self-signed certificate 47
- setup 58
- verify certificate use 73

## T

- tablespace free space 108
- tee command 154
- tempca 44
- tempca command 154
- template files 193
  - customizing 194
- testdbconnection command 155
- threaddumps command 155
- tproc command 156
- troubleshooting
  - database 172
  - general 161
  - logfu 186
  - manager 170
  - partition archiver 168

- SSL 173
- turbo mode 84

## U

- uninstallservice command 156
- users
  - re-enabling account 80

## V

- velocity templates
  - notification 191

## W

- webserver command 157
- webserver-no-wrapper command 157
- webserversetup command 157
- webserversvc command 157
- websetup command 158
- whois
  - command 158