

Installation and Configuration Guide

ArcSight ESM™ 6.0c
with CORR-Engine

October 10, 2012



Installation and Configuration Guide, ArcSight ESM 6.0c

Copyright © 2012 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.

Revision History

Date	Product Version	Description
10/10/2012	ArcSight ESM with CORR-Engine v6.0c	New Document

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: What is ESM with CORR-Engine Storage?	7
ESM Components	7
ArcSight Manager	7
ArcSight CORR-Engine	8
ArcSight SmartConnectors	8
ArcSight Console	8
Deployment Overview	8
ESM Communication Overview	8
Effect on Communication when Components Fail	9
Choosing between FIPS Mode or Default Mode	9
Mode Comparison	10
Using PKCS#11	10
Import Control Issues	10
Chapter 2: Installing ESM	13
System Requirements	13
Supported Platforms	14
Before you Install ESM	14
Keep these TCP ports Open	14
Preparing to Install	14
The /tmp Directory Size	14
Sizing Guidelines for CORR-Engine	15
Create "arcsight" User	15
Increase User Process Limit	16
/opt/arcsight Directory	16
Change /opt/arcsight/ to xfs Format	16
Write and Execute Permission for /opt/arcsight/	16
Installing ESM	17
Running the Installation File	17
Rerunning the Suite Installer	20
Running the First Boot Wizard in Console Mode	20
Configuration	21
Changing the Manager Heap Size	28
Rerunning the Wizard	28

Uninstalling ESM	29
Resource Migration	29
To Set Up ESM Reports to Display in a Non-English Environment	30
On the Manager	30
On the Console	30
The Next Steps	30
Chapter 3: Installing ArcSight Console	33
Console Supported Platforms	33
Required Libraries on the RHEL 6.2 64 Bit Workstation	33
Using a PKCS#11 Token	34
Installing the Console	34
Character Set Encoding	36
Configuration Settings	36
Selecting the Mode in which to Configure ArcSight Console	37
Manager Connection	38
Authentication	40
Web Browser	41
Importing the Console's Certificate into the Browser	44
Starting the ArcSight Console	44
Logging into the Console	46
Reconnecting to the ArcSight Manager	46
Reconfiguring the ArcSight Console	47
Uninstalling the ArcSight Console	47
Chapter 4: Using SmartConnectors	49
Installing the SmartConnector	49
Importing the Manager's Certificate	49
Using keytoolgui to Import Manager's Certificate	50
Exporting the Manager's Certificate	50
Importing the Manager's Certificate into the SmartConnector's Truststore	52
Appendix A: Troubleshooting	57
Location of Log files for Components	57
If you Encounter an Unsuccessful Installation	59
Customizing ESM Components Further	59
Fatal Error when Running the First Boot Wizard	60
Changing the IP Address of your machine	61
Changing the Host Name of the Machine After Running the First Boot Wizard	62
Appendix B: Default Settings for Components	65
General	65
CORR-Engine	65

ArcSight Manager	66
ArcSight Web	67
Appendix C: Using the PKCS#11 Token	69
What is PKCS?	69
PKCS#11	69
PKCS#12	69
PKCS#11 Token Support in ESM	70
References to <ARCSIGHT_HOME>	70
Setting Up to Use a CAC Card	70
Install the CAC Provider's Software	70
Map a User's External ID to the CAC's Subject CN	71
Obtain the CAC's Issuers' Certificate	73
Extract the Root CA Certificate From the CAC Certificate	74
Import the CAC Root CA Certificate into the Manager	76
FIPS Mode - Import into the ESM Manager's nssdb	76
Default Mode - Import into the Manager's Truststore	76
Select Authentication Option in Console Setup	77
Logging in to the Console Using CAC	78
Logging in to the Management Console Using CAC	79
Using CAC with ArcSight Web	80
Appendix D: ESM in FIPS Mode	81
What is FIPS?	81
Network Security Services Database (NSS DB)	82
What is Suite B?	82
NSS Tools Used to Configure Components in FIPS Mode	83
TLS Configuration in a Nutshell	83
Understanding Server Side Authentication	83
Understanding Client Side Authentication	84
Setting up Authentication on ArcSight Web - A Special Case	84
Exporting the Manager's certificate for Other Clients	84
References to ARCSIGHT_HOME	85
Using PKCS #11 Token With a FIPS Mode Setup	85
Installing ArcSight Console in FIPS Mode	85
Connecting a Default Mode Console to a FIPS 140-2 Manager	90
Connecting a FIPS Console to FIPS Enabled Managers	90
Configure Your Browser for FIPS	90
Installing SmartConnectors in FIPS mode	91
How do I Know If My Installation is FIPS Enabled?	91
Index	93

What is ESM with CORR-Engine Storage?

ESM is a Security Information and Event Management (SIEM) solution that collects and analyzes security data from heterogeneous devices on your network and provides you a central, real-time view of the security status of all devices of interest to you.

ESM components gather and store events generated by the devices you identify. These events are filtered and correlated with events from other devices or collection points to discover risks and assess vulnerabilities.

ESM uses the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) Storage, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches. This provides a number of benefits, including increased performance, ease of management, and use of less disk space.

This chapter covers the following topics:

["ESM Components" on page 7](#)

["Deployment Overview" on page 8](#)

["ESM Communication Overview" on page 8](#)

ESM Components

The ESM system comprises of the following components:

- ArcSight Manager
- ArcSight CORR-Engine (Correlation Optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Web
- Management Console
- ArcSight SmartConnectors

ArcSight Manager

ArcSight Manager is at the center of the ESM. The Manager is a software component that functions as a server that receives event data from Connectors and correlates and stores them in the database. The Manager also provides advanced correlation and reporting

capabilities. The Manager and CORR-Engine are integrated components and get installed on the same machine.

ArcSight CORR-Engine

ArcSight CORR-Engine is a long term data storage and retrieval engine that enables the product to receive events at high rates. The Manager and CORR-Engine are integrated components and get installed on the same machine.

ArcSight SmartConnectors

SmartConnectors are software components that forward security events from a wide variety of devices and security event sources to ArcSight CORR-Engine. SmartConnectors are not bundled with ESM and should be separately installed.

ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks, such as fine tuning the ESM content and managing users. The ArcSight Console is not bundled with ESM and should be separately installed.

Deployment Overview

The following is an example of how various ArcSight components are normally deployed in a network.

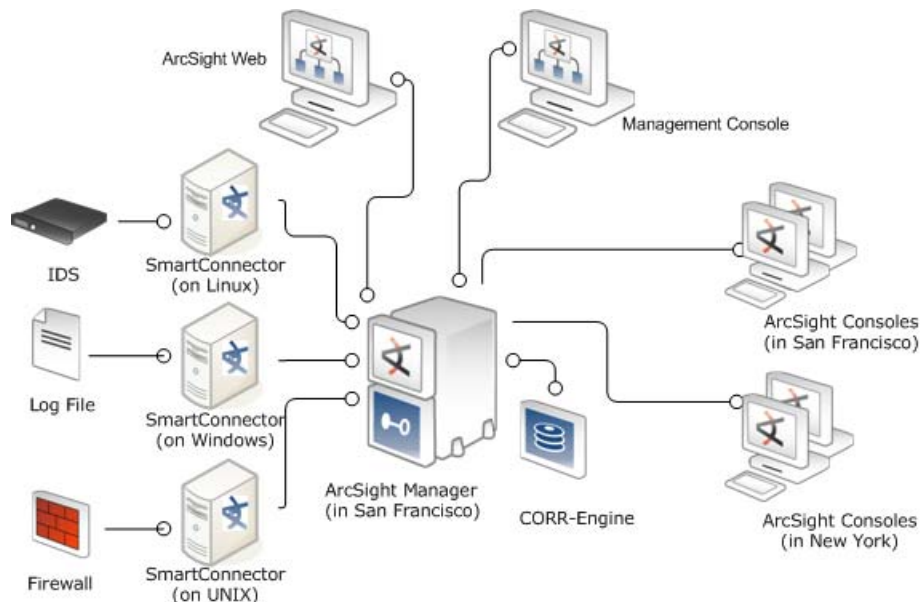


Figure 1-1 ESM Deployment

ESM Communication Overview

ArcSight Console, ArcSight Manager, and ArcSight SmartConnector communicate using HTTP (HyperText Transfer Protocol) over SSL (Secure Sockets Layer), often referred to as HTTPS (HyperText Transfer Protocol Secure). The HTTPS protocol provides for data encryption, data integrity verification, and authentication for both server and client.

SSL works over TCP (Transport Control Protocol) connections. The default incoming TCP port on ArcSight Manager is 8443.

The Manager never makes outgoing connections to the Console or SmartConnectors. The Manager connects to the CORR-Engine through a loopback interface using a propriety protocol.

Effect on Communication when Components Fail

If any one of the software components is unavailable, it can affect communication between other components.

If the CORR-Engine is unavailable for any reason, the Manager stops accepting events and caches any events that were not committed to the CORR-Engine. The SmartConnectors also start caching new events they receive, so there is no event data loss. The Console gets disconnected.

When the CORR-Engine is filled to capacity, as new events come in the Manager starts deleting existing events starting from the oldest dated event.

If the Manager is unavailable, the SmartConnectors start caching events to prevent event data loss. The CORR-Engine is idle. The Console is disconnected.

If a SmartConnector fails, whether event data loss will occur or not depends on the SmartConnector type. SmartConnectors that listen for events from devices such as the SNMP SmartConnectors will stop accepting events. However, a SmartConnector that polls a device, such as the NT Collector SmartConnector, may be able to collect events that were generated while the SmartConnector was down, once the SmartConnector comes back up.

Choosing between FIPS Mode or Default Mode

ESM supports the Federal Information Processing Standard 140-2(FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet these standards.

Depending on your requirements, you can choose to install the ESM components in either of these modes:

- Default mode (standard cryptography)
- FIPS 140-2 mode
- FIPS with Suite B mode

Mode Comparison

The following table outlines some of the basic differences between the three modes that ESM supports:

Mode	Use of SSL/TLS	Default Cipher Suites	Keystore/Truststore
Default Mode	SSL	<ul style="list-style-type: none"> TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA More... 	Keypair and Certificates stored in Keystore and cacerts, and Truststore in JKS format
FIPS 140-2 Mode	TLS	<ul style="list-style-type: none"> TLS_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA 	Keypair and Certificates stored in NSSDB
FIPS with Suite B Mode	TLS	<ul style="list-style-type: none"> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA Suite B 128 bits security level, providing protection from classified up to secret information TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA Suite B 192 bits security level, providing protection from classified up to top secret information 	Keypair and Certificates stored in NSSDB

Using PKCS#11

ESM supports the use of a PKCS#11 token such as the Common Access Card (CAC) to log into the Console or ArcSight Web. PKCS#11 is Public-Key Cryptography Standard (PKCS), published by RSA Laboratories which describes it as “a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.”

You can use the PKCS#11 token to log in regardless of the mode in which ArcSight Console or ArcSight Web is running, in FIPS 140-2 mode or default mode.

Import Control Issues

If you are a customer in the United States, you can skip reading this section. If you are a customer outside of the United States, you need to be aware of your country's restrictions on allowed cryptographic strengths. The embedded JRE in ArcSight components, ship with the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files and they are enabled by default. These files are:

- jre\lib\security\local_policy.jar
- jre\lib\security\US_export_policy.jar

This is appropriate for most countries. However, if your government mandates restrictions, you should backup the above two *.jar files and use the restricted version files instead. They are available at:

jre\lib\security\local_policy.jar.original

jre\lib\security\US_export_policy.jar.original

You will have to rename *.jar.original to *.jar.

The only impact of using the restricted version files would be that you will not be able to use ArcSight's keytoolgui to import unrestricted strength key pairs. Also, you will not be able to save the keystore if you use passwords that are longer than four characters. No other ESM functionality is impacted.

Chapter 2

Installing ESM

This chapter covers the following topics:

- [“System Requirements” on page 13](#)
- [“Before you Install ESM” on page 14](#)
- [“Preparing to Install” on page 14](#)
- [“Installing ESM” on page 17](#)
- [“Uninstalling ESM” on page 29](#)
- [“Resource Migration” on page 29](#)
- [“To Set Up ESM Reports to Display in a Non-English Environment” on page 30](#)
- [“The Next Steps” on page 30](#)

We recommend that you read the ESM *Release Notes* before proceeding further.

System Requirements

The hardware requirements for ESM 6.0c are as follows:

	Minimum Required	Recommended	High Performance
Processors	8 cores	16 cores	32 cores
Memory	36 GB RAM	64 GB RAM	128 GB RAM
Hard Disk	250 GB disk space (RAID 10) 15,000 RPM	1.5 TB disk space (RAID 10) 15,000 RPM	<= 8 TB (RAID 10) 15,000 RPM



The “Minimum Required” values applies to systems running base system content at low EPS (typical in lab environments). It should not be used for systems running high number of customer-created resources, or for systems that need to handle high event rates. Please use the “Recommended” or “High Performance” specifications for production environments that will be handling sizable EPS load with additional content and user activity.

Using Pattern Discovery or large numbers of Assets and Actors puts additional load on the system that can reduce the search and event processing performance. For further assistance in sizing your ESM installation, contact HP ArcSight Customer Support.

Supported Platforms

ESM 6.0c is supported on Red Hat Enterprise Linux 6.2 64-bit platform that has been installed using at least the "Basic Server" option with added "compatibility libraries" at the time of installation. Refer to the Product Lifecycle document available on the Protect 724 site for further information on supported platforms and browsers.

If you would like to install the product in GUI mode, you will also need to install X Window system package on your machine if it does not already exist.

Before you Install ESM

Before you begin to install ESM, do the following:

- The ESM 6.0c installation package is available for download from the HP Software Depot at <http://support.openview.hp.com/downloads.jsp>. Download the [ArcSightESMSuite-xxxx.tar](#) file and copy it on to the system where you will be installing ESM. The xxxx in the file name stands for the build number.
- Once you have downloaded the .tar file from the HP Software Depot, initiate license procurement by following the instructions in the Electronic Delivery Receipt you receive from HP in an email after placing the order.



- You do not need to unzip the license zip file. ESM recognizes the license file in the zipped state.
 - Make sure that the [ArcSightESMSuite-xxxx.tar](#) file is owned by the user "arcsight".
-

- Copy the [xfsprogs-3.1.1-6.el6.x86_64.rpm](#) file from your Linux installation CD to the machine where you will be installing ESM.

Keep these TCP ports Open

Before installing ESM, open the following TCP ports on your system if not already open and ensure that no other process is using these TCP ports:

Open the following TCP ports for external incoming connections:

8443

9443

The following TCP ports are used internally for inter-component communication by ESM:

1976, 2812, 3306, 5555, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8765, 8808, 8880, 8881, 8888, 8889, 9000, 9123, 9124, 9999, 45450

Preparing to Install

Before you run the installation file, you must prepare your system.

The /tmp Directory Size

Make sure that your **/tmp** directory has at least 3 GB of space.

Sizing Guidelines for CORR-Engine

When installing ESM 6.0c, the CORR-Engine storage sizes are automatically calculated based on your hardware per the default values in the table below. These are the recommended sizing guidelines. You can change any of the default storage sizes in the “CORR-Engine Configuration” panel of the wizard, but when doing so, be sure that you take the minimum and maximum values allowed into consideration.

System Storage - non-event storage, for example, resources, trends, and lists

Event Storage - storage for events

Online Event Archive - archive of online events

Available Space - the available space on your machine. ESM automatically detects it for your machine.

Reserved Space - used for system internal use. This is calculated as either 10% of available space or 10 GB whichever is greater.

Usable Space - calculated as Available Space minus Reserved Space.

	Recommended	Minimum	Maximum
System Storage Size	One-sixth of usable space	3 GB	500 GB
Event Storage Size	Four-sixths of usable space	5 GB	8 TB
Online Event Archive Size	Remaining space after the System and Event storage have been allocated	1 GB	No limit



Important!

The sum of space allotted to system storage, archive storage and online event storage should not exceed usable space (90%).

Create “arcsight” User

While logged in as user “root”, create a new user called “arcsight” by entering the following commands in a terminal:

```
groupadd arcsight
```

```
useradd -c "arcsight_software_owner" -g arcsight -d /home/arcsight -m -s /bin/bash arcsight
```

Change the password for user “arcsight”:

```
passwd arcsight
```

Enter a new password when prompted and reenter it when prompted to confirm.

Increase User Process Limit

On the Red Hat 6.2 platform, the default user process limit is 1024. This may cause an error when the Manager tries to create more threads.

To ensure that the system has adequate processing capacity, increase this default limit, while logged in as user "root":

- 1 Edit `/etc/security/limits.d/90-nproc.conf` file to change or append the following entries:



Be sure to include the `*` in the lines below. It is important that you add all of the following entries exactly as specified below. Any omissions will lead to your system experiencing runtime errors.

```
* soft nproc 10240
* hard nproc 10240
* soft nofile 65536
* hard nofile 65536
```

- 2 Reboot the machine.
- 3 Log in as user "arcsight".
- 4 Run the following command to verify the new settings:

```
ulimit -a
```

- 5 Verify that the output shows the following values for Open files and Max user processes:

```
open files      65536
max user processes 10240
```

/opt/arcsight Directory

ESM 6.0c gets installed in `/opt/arcsight/`. If the `/opt/arcsight/` directory does not exist, create it while logged in as a 'root' user.

Change /opt/arcsight/ to xfs Format

If not already in xfs format, ArcSight recommends changing `/opt/arcsight/` to the xfs format for optimum performance. To do so:

- 1 Log in as user "root" if you have not already done so.
 - 2 Run the following command to install the xfsprogs RPM:
- ```
rpm -i xfsprogs-3.1.1-6.el6.x86_64.rpm
```
- 3 Mount the partition containing `/opt/arcsight/` with `inode64` option.

## Write and Execute Permission for /opt/arcsight/

Make sure that the user "arcsight" has write and execute permission for the `/opt/arcsight/` directory.



Change the owner and group of `/opt/arcsight/` to 'arcsight' user and group by issuing the following commands:

```
chown arcsight:arcsight /opt/arcsight
```

## Installing ESM



- Using an ssh -X session to run the ESM 6.0c installation file causes errors and the wizard does not complete. Instead of using ssh -X to run the installation wizard, use ssh to connect to the machine where you will be installing ESM 6.0c and set your DISPLAY environment variable to point to a valid X11 display.
- Spaces in directory names appearing within paths are not supported.

**1** Untar the tar file in order to obtain the installation file. To do so:

- a Log in as user "arcsight".
- b Transfer the license file and the .tar file to this machine where you will be installing ESM.
- c Change directory to the location where you downloaded the tar file.
- d Make sure that the tar file is owned by the user "arcsight".
- e Run the following command to untar the file:

```
tar xvf ArcSightESMSuite-xxxx.tar
```

**2** If not already granted, give the `ArcSightESMSuite.bin` file the execute permission. To do so enter:

```
chmod +x ArcSightESMSuite.bin
```

## Running the Installation File

While logged in as user "arcsight" do the following:

**1** Run the installation file as follows:

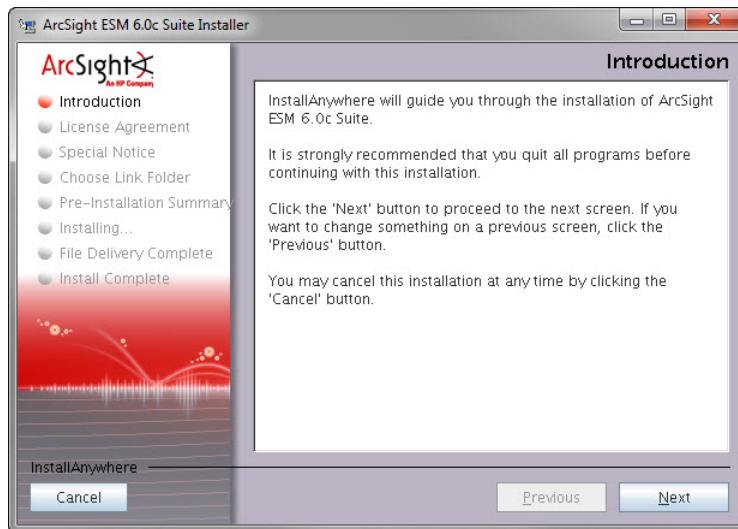
```
./ArcSightESMSuite.bin
```

The installation wizard opens.

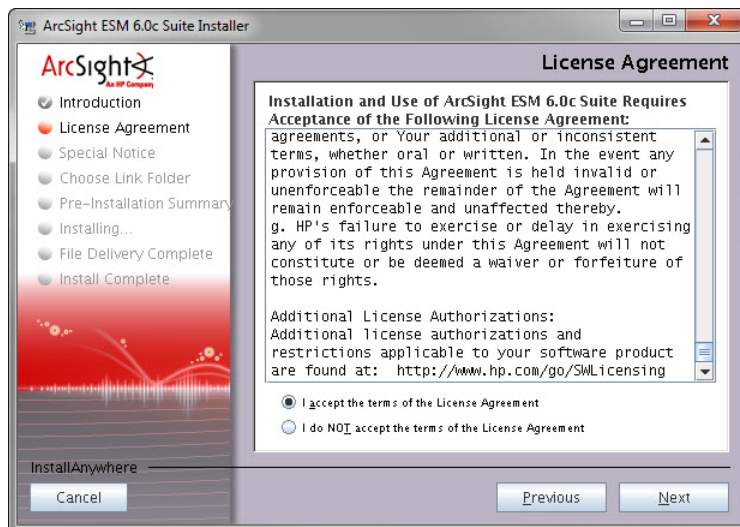


- If you are installing in console mode, be aware that the installation bits install without confirmation of progress. Product components get installed silently and the system displays the message, "File Delivery Complete" after the bits are successfully installed.
- Make sure that X Window is not running when running the first boot wizard in console mode.

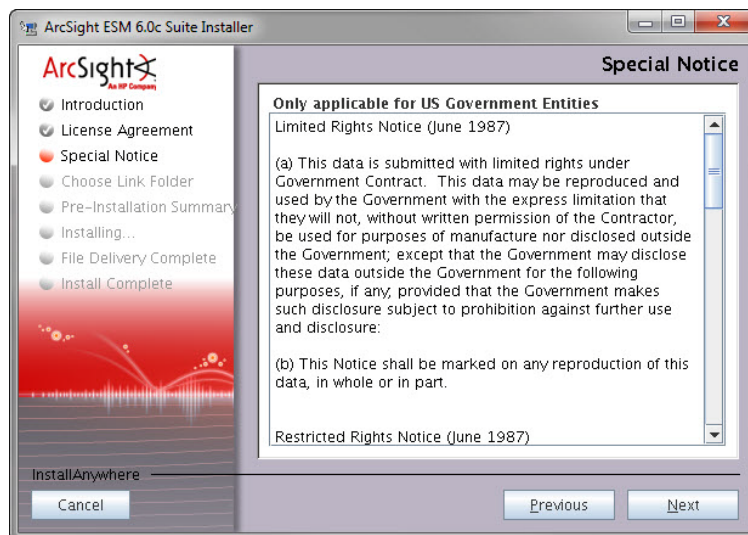
- 2 Read the introductory message and click **Next**.



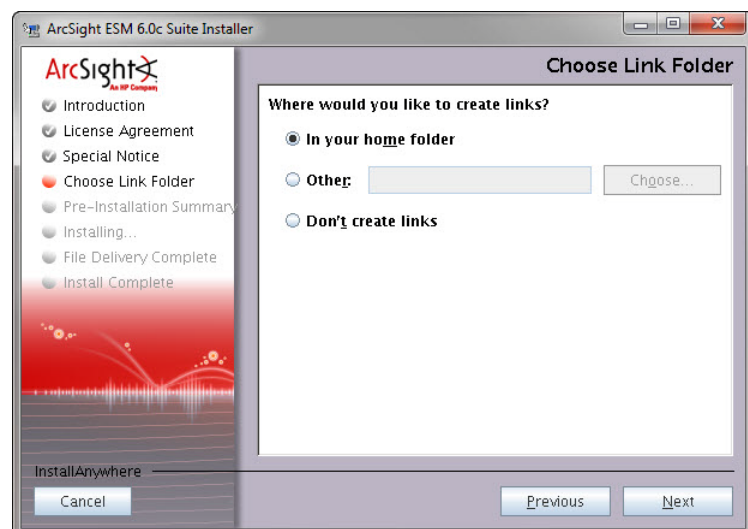
- 3 The "I accept the terms of the License Agreement" radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read the License Agreement click the **I accept the terms of the License Agreement** radio button and click **Next**.



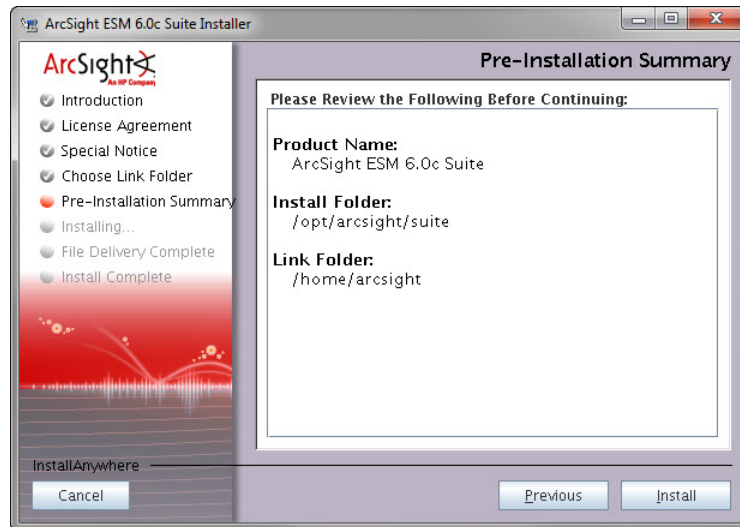
- 4 Read the special notice and click **Next**.



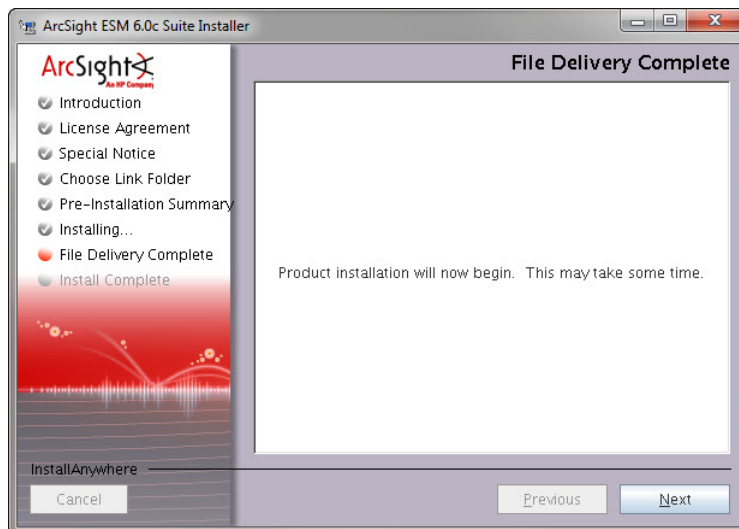
- 5 Select the location where you would like the installer to place the links for the installation and click **Next**.



- 6 Review the summary in the Pre-Installation screen. If need be, click **Previous** to make any changes. When you are ready to proceed, click **Install**.



- 7 The installer first places all the installation files in the appropriate folders and when it is done, you will get a File Delivery Complete screen. Click **Next**.



The installer installs each component. After the installation completes, the configuration screen opens.

## Rerunning the Suite Installer

If your installation is interrupted before you get to the "File Delivery Complete" screen and your installation process exits for any reason (for instance, you abort it), you can rerun the installer. Before you do so, make sure that you have removed all `install.dir.XXXXX` directories from the `/tmp` directory. Also, be sure to delete all directories and files that were created by the installer in the `/opt/arcsight` directory.

## Running the First Boot Wizard in Console Mode

If you are installing the product in console mode, start the installation manually by issuing the following command:

```
/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
```

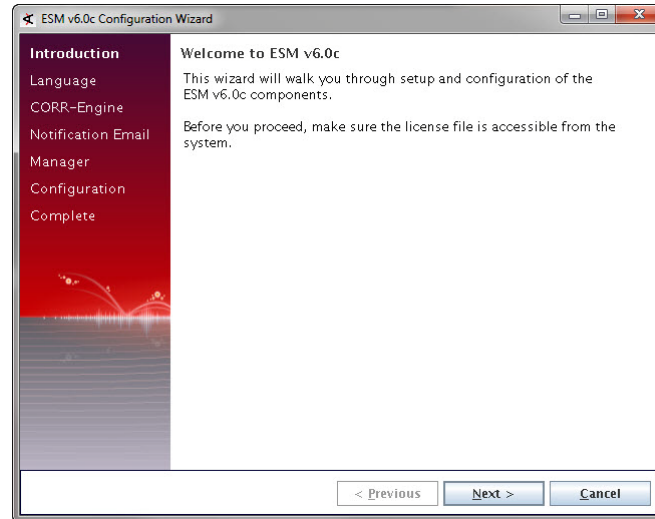
**Note**

Make sure that X-Windows is not running when running the first boot wizard in console mode.

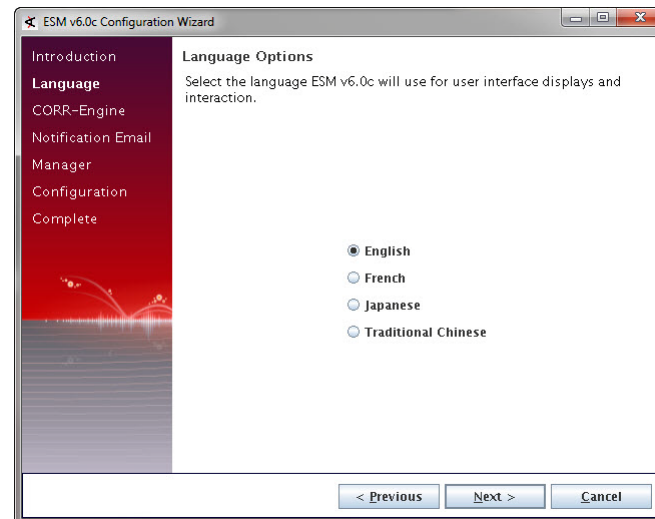
## Configuration

Once the installation completes, the configuration wizard to configure the ESM components opens.

- 1 Read the Welcome screen and click **Next**.



- 2 Select the language for interface displays and click **Next**.



- 3 Set a password for the CORR-Engine and reenter it in the Password confirmation text box and click **Next**. For information on password restrictions see the *Administrator's Guide* for ESM, chapter "Configuration", section "Managing Password Configuration".

- 4 Enter the CORR-Engine storage allocation information and click **Next**.



- The maximum event storage size allowed is 8TB. If you exceed this limit, you will need to store data offline.
- You can disable archiving if need be from the Management Console after you have installed ESM. Refer to the *Management Console User's Guide* for information on how to do so.

- 5 Configure the following e-mail addresses:

**Notification e-mail address:** An e-mail address of the person who should receive e-mail notifications in the event that the ArcSight Manager goes down or encounters some other problem.

**From e-mail address:** E-mail address that will be used to represent the sender of the e-mail notifications.

Click **Next**.

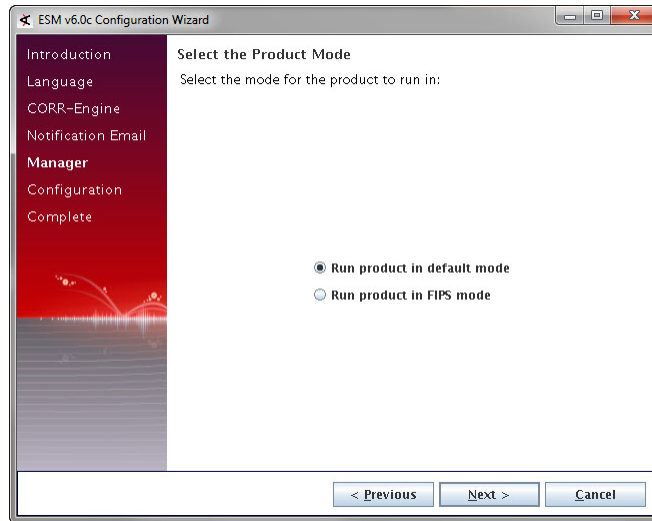
- 6 Enter the location of the license file you downloaded. Alternatively, you can browse to the file and click **Next**.



**Note**

If you have a valid existing ESM license, you can use it with ESM 6.0c.

- 7 Select whether you want to install ESM in default mode or FIPS mode.



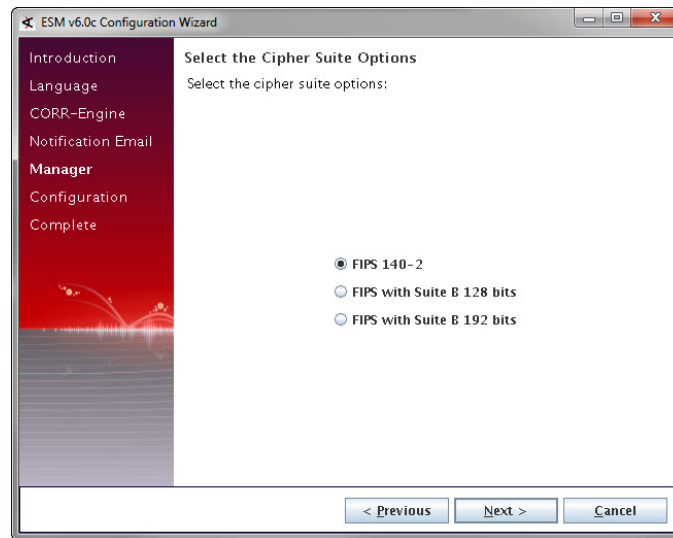
Click **Next**.



- If you choose to install the product in FIPS mode, be sure to install the Console in FIPS mode too. Refer to [“Installing ArcSight Console in FIPS Mode” on page 85](#) for instructions on installing the Console in FIPS mode.
  - Once you have configured the software in FIPS-140 mode, you will not be able to convert it to default mode without reinstalling it.
  - Converting from default mode installation to FIPS 140-2 mode is supported. If you need to do so at any time, refer to the *Administrator's Guide* for instructions to do so.
  - By default, ESM uses a self-signed certificate. If you would like to use a CA-signed certificate, you will have to import the CA-signed certificate manually **after** the configuration wizard completes successfully. Refer to the *Administrator's Guide* for ESM for details on using a CA-signed certificate.
-

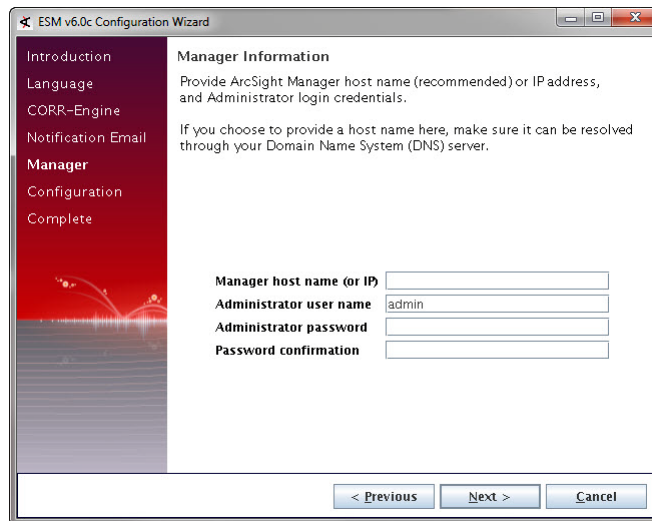


- 8 (If you selected FIPS mode only)** You will see a screen asking you to select the cipher suite.



Suite B defines two security levels of 128 and 192 bits. The two security levels are based on the Advanced Encryption Standard (AES) key size that is used instead of the overall security provided by Suite B. At the 128-bit security level, the 128 bit AES key size is used. However, at the 192-bit security level, a 256 bit AES key size is used. Although, a larger key size would mean more security, it would also mean computational cost in terms of time and resource (CPU) consumption. In most scenarios, the 128-bit key size is sufficient.

- 9 Enter the Manager's hostname or IP address and set a password for the admin user and click **Next**.



The screenshot shows the 'ESM v6.0c Configuration Wizard' window. On the left is a vertical navigation pane with the following items: Introduction, Language, CORR-Engine, Notification Email, **Manager** (highlighted in red), Configuration, and Complete. The main area is titled 'Manager Information' and contains the following text: 'Provide ArcSight Manager host name (recommended) or IP address, and Administrator login credentials.' and 'If you choose to provide a host name here, make sure it can be resolved through your Domain Name System (DNS) server.' Below this text are four input fields: 'Manager host name (or IP)', 'Administrator user name' (with 'admin' entered), 'Administrator password', and 'Password confirmation'. At the bottom of the window are three buttons: '< Previous', 'Next >', and 'Cancel'.

**Caution**

Manager host name is the local host name or IP address of the machine where the Manager gets installed. Note that this name is what all clients (for example, ArcSight Console) will need to specify to talk to the ArcSight Manager. Using a host name instead of an IP address is recommended for flexibility.

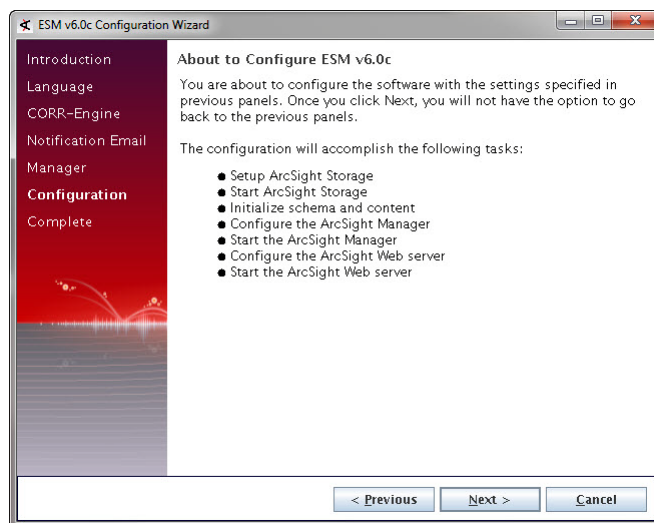
The Manager host name will be used to generate a self-signed certificate. The Common Name (CN) in the certificate will be the Manager host name that you specify in this screen.

Although the Manager uses a self-signed certificate by default, you can switch to using a CA-signed certificate if needed. This can be done post installation. Refer to the *ESM Administrator's Guide* for instructions.

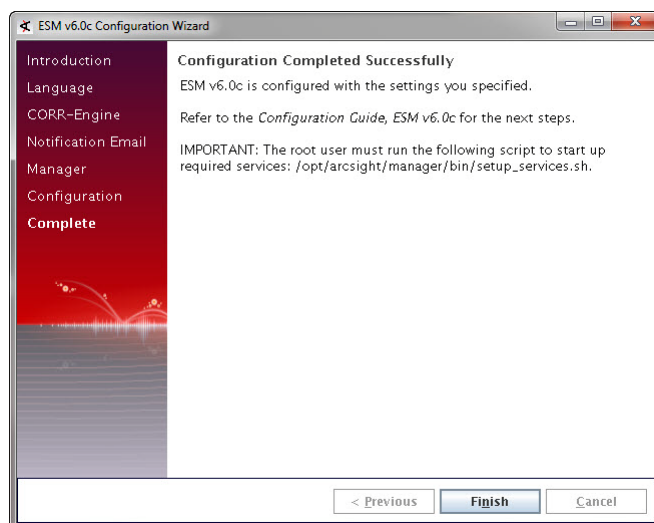
- 10 The next screen informs you of the steps that will take place in order to configure ESM. Read it and click **Next**.

**Caution**

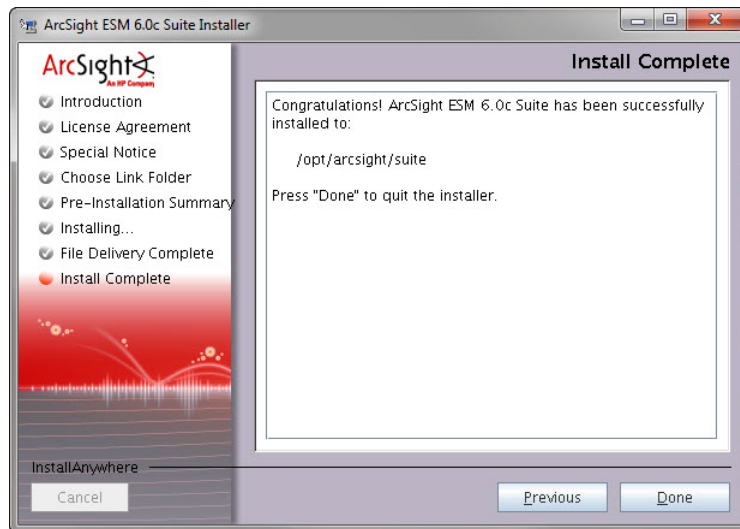
Review the selections you made in the previous screens of this wizard and make sure that they are to your satisfaction. Once you click Next, the product is installed as specified and cannot be changed.



- 11** Upon successful configuration, you will see the Configuration Completed Successfully screen. Click **Finish**.



- 12 Click **Done** in the Install Complete screen.



### Important!

- 13 Log in user “root” and run the following script to set up the required services:



This step is required in order to start the services.

```
/opt/arcsight/manager/bin/setup_services.sh
```

- 14 If you would like to migrate your resources from an existing (legacy) ESM installation, you should do so now. Contact HP ArcSight Customer Support for further instructions.

## Changing the Manager Heap Size

If you need to change the Manager’s heap size after the installation completes, you can do so from the Management Console. Refer to the Management Console User’s Guide, chapter “Administration”, section, “Configuration Management”.

## Rerunning the Wizard

The wizard can be rerun manually only if you exit it at any point **before** you reach the first configuration screen called “About to Configure ESM v6.0c” ([Step 10 on page 26](#)).

If for any reason you cancel out of the wizard or run into an error before the configuration screen, you can re-run the wizard manually after cancellation or error-out.

- 1 To rerun the wizard run:

```
rm /opt/arcsight/manager/config/fbwizard*
```

- 2 To run the First Boot Wizard, run the following from the `/opt/arcsight/manager/bin` directory while logged in as user “arcsight”:

### In GUI mode

```
./arcsight firstbootsetup -boxster -soft
```

### In console mode

```
./arcsight firstbootsetup -boxster -soft -i console
```



Make sure that X-Windows is not running when running the first boot wizard in console mode.

If you encounter a failure during the configuration stage, you will need to uninstall the product and reinstall it.

## Uninstalling ESM

To uninstall ESM,

- 1 Log in as user "root".
- 2 Run the following command:

```
/opt/arcsight/manager/bin/remove_services.sh
```

- 3 Log in as user "arcsight".
- 4 Shutdown any "arcsight" processes that are not already down.
- 5 Run the uninstaller program from either the directory where you have created the links while installing the product or if you had opted not to create links, then run this from the `/opt/arcsight/suite/UninstallerData` directory:

```
./Uninstall_ArcSight_ESM_Suite
```

Alternatively, you can run the following command from the `/home/arcsight` (or wherever you installed the shortcut links) directory:

```
./Uninstall_ArcSight_ESM_Suite_6.0
```

- 6 Verify that the `/tmp` and `/opt/arcsight` directories contain no ESM-related files. If that is not the case:
  - a While logged in as user "arcsight", kill all arcsight processes.
  - b Delete all remaining arcsight-related files/directories in `/opt/arcsight/` and `/tmp` directory manually.
  - c Delete any links created during installation.

## Resource Migration

If you would like to migrate your resources from an existing (legacy) ESM installation, you should do so on a freshly installed ESM on which resources have not been altered or added. Any resources that are changed or added after installation along with their associations with any events will be wiped out while migrating the resources.

Once you have installed the ESM 6.0c software, if you would like to migrate your resources from a legacy ESM installation, contact HP for assistance to do so.

## To Set Up ESM Reports to Display in a Non-English Environment

To enable international characters in string-based event fields to be retrieved by queries, you need to store such characters correctly. Following the processes in this section will allow the international characters to be stored and recognized correctly by ESM.

### On the Manager

This procedure is required only if you plan to output reports that use international characters in PDF format. You will need to purchase the [ARIALUNI.TTF](#) font file.

- 1 On the Manager host, place the font file [ARIALUNI.TTF](#) in a folder. For example:  

```
/usr/share/fonts/somefolder
```
- 2 Modify the ESM reports properties file, [sree.properties](#), located in `/opt/arcsight/manager/reports/` directory by default.  
Add the following line:  

```
font.truetype.path=/usr/share/fonts/somefolder
```
- 3 Restart the Manager by running:  

```
/sbin/service arcsight_services restart manager
```
- 4 In the ArcSight Console UI, select the Arial Unicode MS font in all the report elements, including the report template.

### On the Console

Set preferences in the Console and on the Console host.

- 1 Install the Arial Unicode MS font on the Console host operating system if not already present.
- 2 Edit the following script located in `<ARCSIGHT_HOME>/current/bin/scripts` directory by default:

**On Windows:** Edit [console.bat](#)

**On Macintosh:** Edit [console.sh](#)

**On Linux:** No edits required. The coding is set correctly.

Find the section [ARCSIGHT\\_JVM\\_OPTIONS](#) and append the following JVM option:

```
" -Dfile.encoding=UTF8 "
```

- 3 In the ArcSight Console Preferences menu, set Arial Unicode MS as the default font:

Go to **Edit > Preferences > Global Options > Font**

**On Windows:** Select [Arial Unicode MS](#) from the drop-down

**On Linux:** Enter [Arial Unicode MS](#)

## The Next Steps

Download the ArcSight Console and install it on a supported platform. Refer to the chapter, [Installing ArcSight Console](#), for details on how to do this.

You can also access the ArcSight Manager from the Management Console using a browser. To do so, enter the following URL in the browser's address bar:

`https://<Manager's_IP or hostname>:8443`

Refer to the *Management Console User's Guide* for more information on using the Management Console.

Read the *Release Notes* available on the HP ArcSight Customer Support download site.





## Chapter 3

# Installing ArcSight Console

---

The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of ArcSight Web) to ArcSight ESM. This chapter explains how to install and configure the ArcSight Console in default mode. To install the Console in FIPS mode, see [Appendix D, ESM in FIPS Mode, on page 81](#). Section [“Mode Comparison” on page 10](#) lists the basic differences between the three modes.

The following topics are covered in this chapter:

- [“Console Supported Platforms” on page 33](#)
- [“Using a PKCS#11 Token” on page 34](#)
- [“Installing the Console” on page 34](#)
- [“Starting the ArcSight Console” on page 44](#)
- [“Reconnecting to the ArcSight Manager” on page 46](#)
- [“Reconfiguring the ArcSight Console” on page 47](#)
- [“Uninstalling the ArcSight Console” on page 47](#)

Start the Manager and make sure it is running before installing the ArcSight Console. The ArcSight Console may be installed on the same host as the Manager, or on a different machine. Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager.

## Console Supported Platforms

Refer to the Product Lifecycle document available on the Protect 724 site for the most current information on supported platforms and browsers.

## Required Libraries on the RHEL 6.2 64 Bit Workstation

On the RHEL 6.2 64-bit Workstation, the Console requires the following libraries to be installed:

`pam-1.1.1-10.el6.x86_64.rpm`

`pam-1.1.1-10.el6.i686.rpm`

`libXtst-1.0.99.2-3.el6.x86_64.rpm`

`libXtst-1.0.99.2-3.el6.i686.rpm`

```
libXp-1.0.0-15.1.el6.x86_64.rpm
libXp-1.0.0-15.1.el6.i686.rpm
libXmu-1.0.5-1.el6.x86_64.rpm
libXmu-1.0.5-1.el6.i686.rpm
libXft-2.1.13-4.1.el6.x86_64.rpm
libXft-2.1.13-4.1.el6.i686.rpm
libXext-1.1-3.el6.x86_64.rpm
libXext-1.1-3.el6.i686.rpm
gtk2-engines-2.18.4-5.el6.x86_64.rpm
gtk2-2.18.9-6.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.i686.rpm
compat-db-4.6.21-15.el6.x86_64.rpm
compat-db-4.6.21-15.el6.i686.rpm
```

## Using a PKCS#11 Token

ArcSight ESM supports the use of a PKCS#11 token, such as the Common Access Card (CAC), which is used for identity verification and access control. PKCS#11 is a public key cryptography standard which defines an API to cryptographic tokens.

You can use the PKCS#11 token regardless of the mode that the client is running in - with clients running in FIPS 140-2 mode or with clients running in the default mode. See [Appendix C, Using the PKCS#11 Token, on page 69](#) for details on using a PKCS #11 token with the Console.

## Installing the Console



On Macintosh platforms, please make sure that:

- You are using an intel processor based system
- You have the JRE installed on your system before installing the Console. Refer to the Release Notes for the version of JRE to install
- If you are installing the Console on a new system for the first time, or if you have upgraded your system causing the JRE update, your Console installation might fail. To work around this issue, make sure that you change the permissions on the cacerts file to give it write permission before you import it.



A Windows system was used for the sample screens. If you are installing on a Unix based system, you will notice a few Unix-specific screens. Path separators are / for Unix and \ for Windows.

---

**Note**

On Macintosh platform, if your JRE gets updated, you will see the following error when you try to log into the Console:

`IOException: Keystore was tampered with or password was incorrect.`

This happens because the Mac OS update changed the password for the cacerts file in the system's JRE. To work around this issue, before you start the Console, change the default password for the `cacerts` file by setting it to the following in the `client.properties` file (create the file if it does not exist) in the Console's `/current/config` folder by adding:

```
ssl.truststore.password=changeme
```

Make sure that you have the ArcSight Manager installed before installing the ArcSight Console.

To install ArcSight Console, run the self-extracting archive file that is appropriate for your target platform. Go to the directory where the ArcSight Console Installer is located.

| Platform  | Installation File                                     |
|-----------|-------------------------------------------------------|
| Linux     | <code>ArcSight-6.0.x.nnnn.y-Console-Linux.bin</code>  |
| Windows   | <code>ArcSight-6.0.x.nnnn.y-Console-Win.exe</code>    |
| Macintosh | <code>ArcSight-6.0.x.nnnn.y-Console-MacOSX.zip</code> |

- 1 Click **Next** in the Installation Process Check screen.
- 2 Read the introductory text in the Introduction panel and click **Next**.
- 3 The "I accept the terms of the License Agreement" radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read the text click the "I accept the terms of the License Agreement" radio button and click **Next**.
- 4 Read the text in the Special Notice panel and click **Next**.
- 5 Navigate to an existing folder where you want to install the Console or accept the default and click **Next**. If you specify a folder that does not exist, the folder gets created for you.

**Caution**

- On Linux and Macintosh systems, spaces are not supported in install paths for ESM 6.0c.
- **On Windows Vista (64-bit):** Make sure that you have administrative privileges to the C:\, C:\Program Files, and C:\Windows directories because these are protected folders and you will not be able to create files (creating a folder is allowed, but you need administrative privileges to create a file) under them without having administrative privileges. When you try to export a package to one of these protected folders, the Console checks the permissions for the parent folder, and when it tries to write the file, an exception is thrown if the parent folder does not have explicit write permission. As a result, the Console will not be able to export a resource package directly under these folders.

- 6 Select where you would like to create a shortcut for the Console and click **Next**.
- 7 View the summary in the Pre-Installation Summary screen and click **Install** if you are satisfied with the paths listed. If you want to make any changes, use the Previous button to do so.

You can view the installation progress in the progress bar.

## Character Set Encoding

Install the Console on a machine that uses the same character set encoding as the Manager.

If the character encodings do not match, then user IDs and passwords are restricted to using the following characters:

`a-z A-Z 0-9 _@. # $ % ^ & * + ? < > . { } | , ( ) - [ ]`

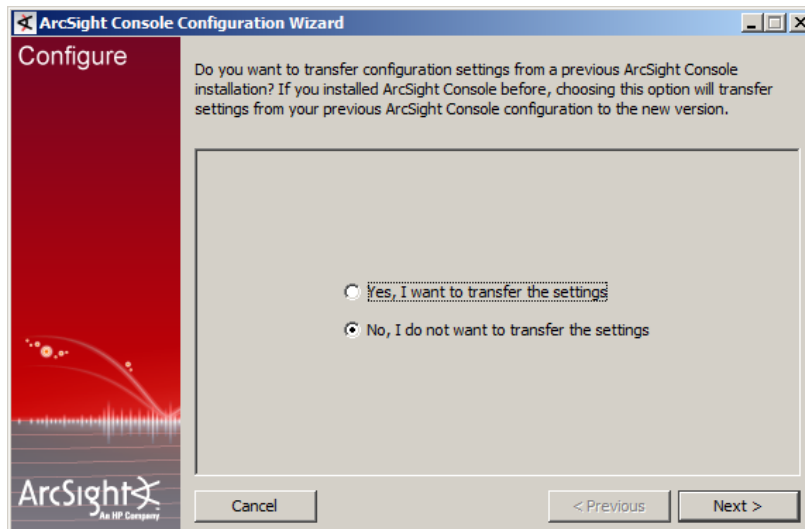
If the Console encoding does not match and a **user ID** contains other characters, That user should not save any custom shortcut key (hot key) schema. The user ID is not properly encoded in the keymap .xml file and that makes it impossible to establish the user's shortcut schema during login. In that circumstance, *all logins fail* on that Console.

If you must use a non-UTF-8 encoding, and you must have user IDs with other characters in them then custom shortcut keys are not supported on any Console where these users would log in. In that situation add the following property to the `console.properties` file: `console.ui.enable.shortcut.schema.persist=false`. This property prevents custom shortcut key schema changes or additions.

If the Console encoding does not match and a **password** contains other characters, that user cannot log in from that Console, as the password hash won't match the one created on the Manager when the password was created.

## Configuration Settings

After the Console has been installed, the wizard asks if you would like to transfer configuration options from an existing installation of ArcSight Console. Choose **No, I do not want to transfer the settings** to create a new, clean installation and click **Next**.

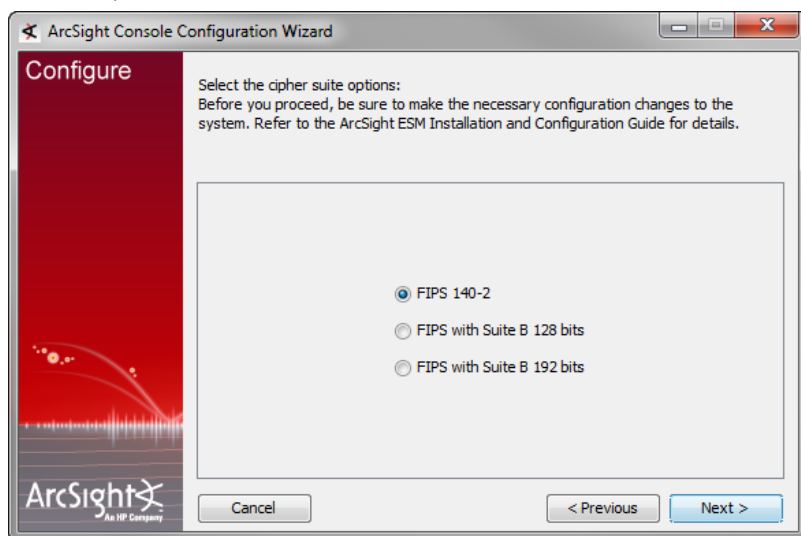


## Selecting the Mode in which to Configure ArcSight Console

Next, you will see the following screen:



Select the mode in which to install the Console. This should be the same mode in which the Manager is installed. If you selected **Run console in FIPS mode**, you will be prompted to select a cipher suite.



Suite B defines two security levels of 128 and 192 bits. The two security levels are based on the Advanced Encryption Standard (AES) key size that is used instead of the overall security provided by Suite B. At the 128-bit security level, the 128 bit AES key size is used. However, at the 192-bit security level, a 256 bit AES key size is used. Although, a larger key size would mean more security, it would also mean computational cost in terms of time and resource (CPU) consumption. In most scenarios, the 128-bit key size is sufficient.

Click **Next**.

## Manager Connection

The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. Enter the host name of the Manager to which the Console will connect.

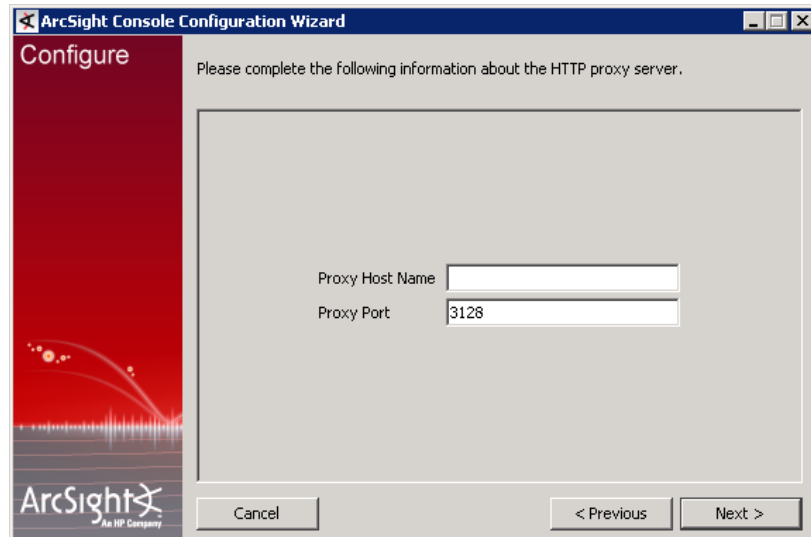


Do not change the Manager's port number.

Click **Next**.

- 8 Select **Use direct connection** option and click **Next**. You can set up a proxy server and connect to the Manager using that server if you cannot connect to the Manager directly.

If you select the Use proxy server option, you will be prompted to enter the proxy server information.



The image shows a screenshot of the 'ArcSight Console Configuration Wizard' window, specifically the 'Configure' step. The window has a title bar with the text 'ArcSight Console Configuration Wizard' and standard Windows window controls. On the left side, there is a red vertical banner with the word 'Configure' at the top and the ArcSight logo at the bottom. The main area of the window is light gray and contains the text 'Please complete the following information about the HTTP proxy server.' Below this text, there are two input fields: 'Proxy Host Name' and 'Proxy Port'. The 'Proxy Port' field has the value '3128' entered. At the bottom of the window, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The 'Next >' button is highlighted, indicating it is the next step in the wizard.

Enter the Proxy Host name and click **Next**.

## Authentication



In order to use PKCS#11 authentication, you must select the Password Based or SSL Client Based authentication method.

The ArcSight Console configuration wizard prompts you to choose the type of client authentication you want to use, as shown in the following screen:



**Password Based and SSL Client Based Authentication** option currently supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method within the **Password Based and SSL Client Based Authentication** option is not currently supported.

If you select **Password Based Authentication**, you will have to login with a user name and password.

If you select **Password Based and SSL Client Based Authentication**, you will be required to enter both user name/password combination and you will be required to setup your client certificate manually. Follow the procedure described in ESM *Administrator's Guide* to set up the client certificate.

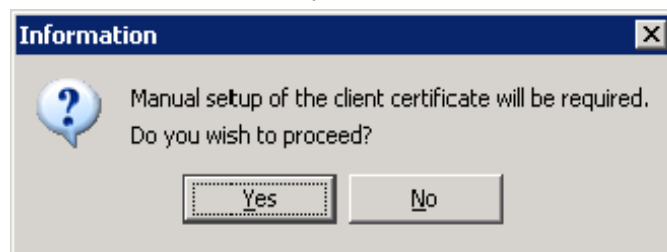


If you selected **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication**, you will be required to select your SSL client based authentication method.



If you plan to use a PKCS #11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the Console, you can refer to [Appendix C, Using the PKCS#11 Token, on page 69](#) for instructions on how to set up the token.

If you select **Client Key Store**, you will see a message reminding you to set up the client certificate after the installation completes.

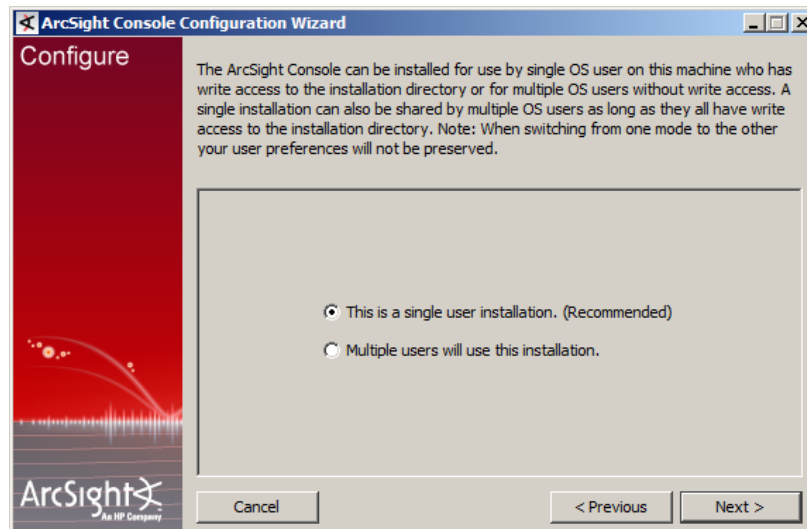
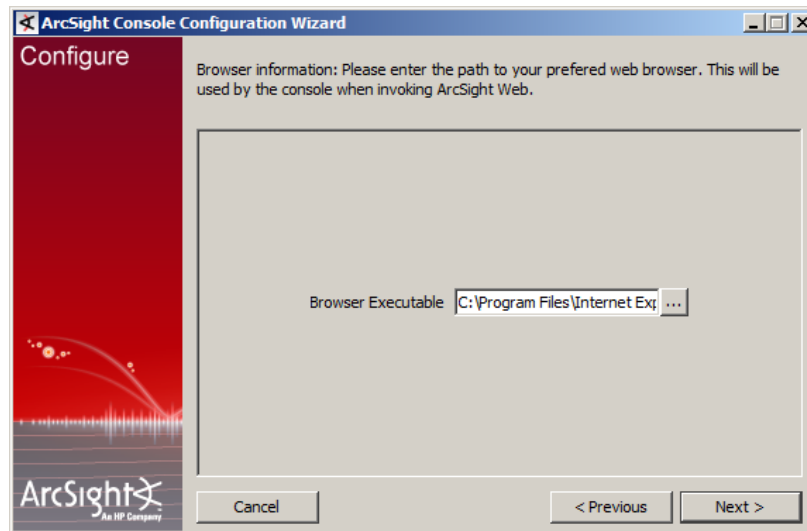


After completing the Configuration Wizard, follow the procedure described in ESM *Administrator's Guide* to set up the client certificate.

## Web Browser

The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Centered Support articles, and other web page content.

Specify the location of the executable for the web browser that you want to use to display the Knowledge Centered Support articles and other web pages launched from the ArcSight Console. Click **Next**.



You can choose from these options:

- This is a single system user installation
  - Select this option when:
    - ◆ There is only one system account on this machine that one or more Console users will use to connect to the Console. For example, a system account, admin, is used by Console users Joe, Jack, Jill, and Jane.

OR

- ◆ All Console users who will use this machine to connect to the Console have their own user accounts on this machine AND these users have write permission to the ArcSight Console's `\current` directory.

**Advantage:** Logs for all Console users are written to one, central location in ArcSight Console's `\current\logs` directory. The user preferences files (denoted by `username.ast`) for all Console users are located centrally in ArcSight Console's `\current`.

**Disadvantage:** You cannot use this option if your security policy does not allow all Console users to share a single system user account or all users to write to the ArcSight Console's `\current` directory.

■ Multiple system users will use this installation

Select this option when:

- ◆ All Console users who will be using this machine to connect to the Console have their own user accounts on this machine

AND

- ◆ These users do not have write permission to the ArcSight Console's `\current\logs` directory.

By selecting this option, each user's log and preferences files are written to the user's local directory (for example, `Document and Settings\username\.arcsight\console` on Windows) on this machine.

**Advantage:** You do not have to enable write permission for all Console users to the Console's `\current` directory.

**Disadvantages:** Logs are distributed. Therefore, to view logs for a specific time period, you will have to access them from the local directory of the user who was connected at that time.

If you do not enable write permission for all the Console users to the Console's `\current` directory, they can only run the following commands (found in the Console's `\bin\scripts`) from the Console command-line interface:

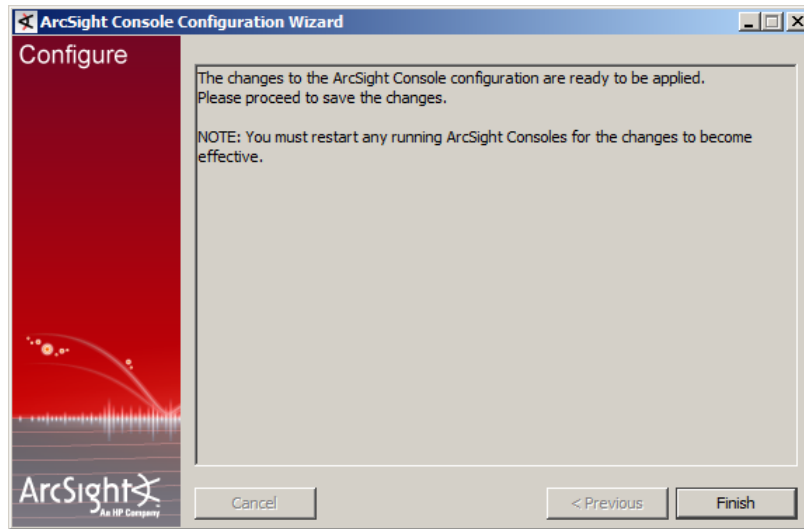
- ◆ `sendlogs`
- ◆ `console`
- ◆ `exceptions`
- ◆ `portinfo`
- ◆ `websearch`

All other commands require write permission to the Console's `\current` directory.



The location from which the Console accesses user preference files and writes logs to depends on the option you select above. Therefore, if you switch between these options after the initial configuration, any customized user preferences may appear to be lost. For example, your Console is currently configured with the "This is a single system user installation" option on a Windows machine. Console user Joe's customized preferences file is located in the Console's `<ARCSIGHT_HOME>\current`. Now, you run the `consolesetup` command and change the setting to Multiple system users will use this installation. Next time Joe connects to the Console, the Console will access Joe's preference file from `Document and Settings\joe\.arcsight\console`, which will contain the default preferences.

You have completed configuring your ArcSight Console. Click **Finish** in the following screen.



Click **Done** in the next screen.



**Note**

**On Mac OS X 10.5 update 8 and later:**

The Mac OS update changed the password for the cacerts file in the system's JRE. Before you start the Console, you need to change the default password for the cacerts file by setting it to the following in the `client.properties` file (create the file if it does not exist) in the Console's `\current\config` folder by adding:

```
ssl.truststore.password=changeme
```

## Importing the Console's Certificate into the Browser

The online help from the Console gets displayed in a browser. Follow these steps in order to view the online help in an external browser if you are using SSL Client Based authentication mode:

- 1 Export the keypair from the Console. You will need to do this using the keytoolgui. Refer to the *Administrator's Guide* for ESM in the "Using Keytoolgui to Export a Key Pair" section.
- 2 Import the Console's keypair into the Browser.

You have installed the ArcSight Console successfully. Please be sure to install any available patches for the Console. Refer to the ArcSight ESM *Patch Release Notes* for instructions on how to install a patch for the Console.

## Starting the ArcSight Console

After installation and setup is complete, you can start ArcSight Console.

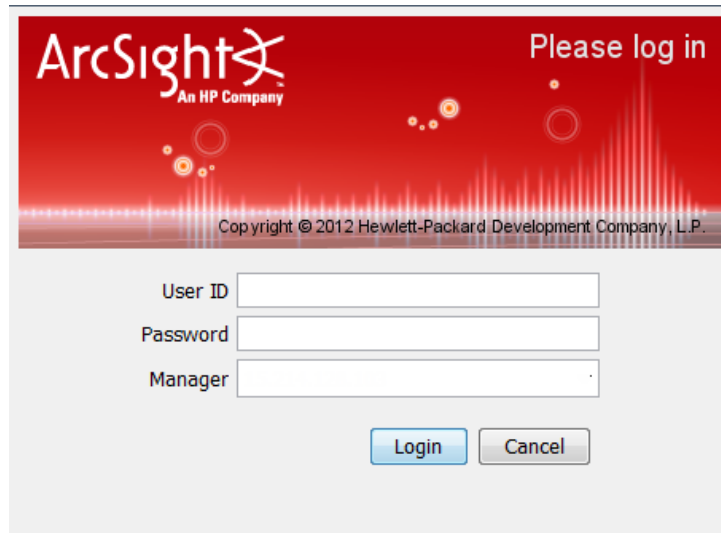
To start the ArcSight Console, use the shortcuts installed or open a command window on the Console's `bin` directory and run:

On Windows:

```
arcsight console
```

On Unix:

```
./arcsight console
```



Depending on the client authentication method you selected when installing the Console, you will see the following buttons on the login screen shown above:

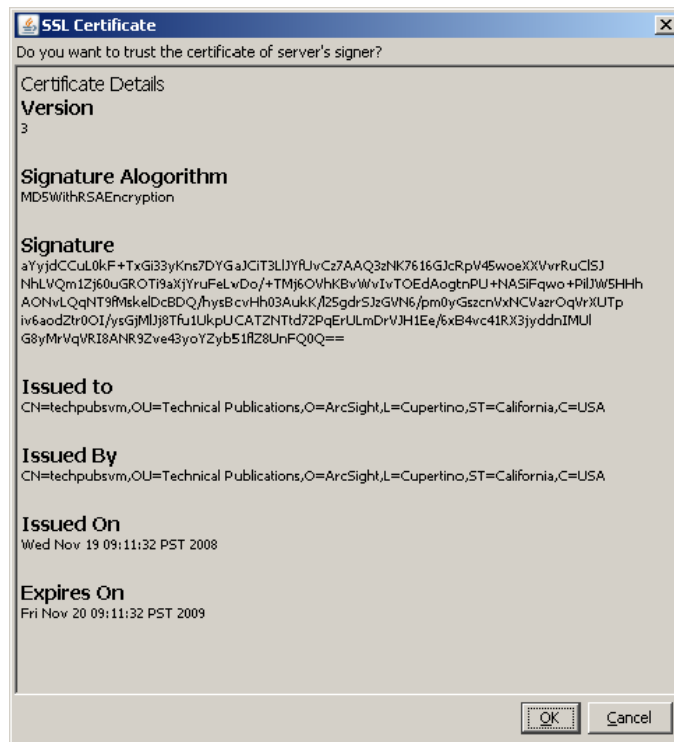
| If you selected...                                 | You will see the following buttons...                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password Based Authentication                      | Login<br>Cancel                                                                                                                                                                                                                                                                                                                                                                   |
| Password Based and SSL Client Based Authentication | Login<br>Cancel                                                                                                                                                                                                                                                                                                                                                                   |
| Password Based or SSL Client Based Authentication  | If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: none"> <li>Login (username and password)</li> <li>SSL Client Login</li> <li>Cancel</li> </ul> If you selected PKCS#11 Token, you will see <ul style="list-style-type: none"> <li>PKCS #11 Login</li> <li>Login</li> <li>Cancel</li> </ul>                                 |
| SSL Client Only Authentication                     | If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: none"> <li>Login (username and password). This option is disabled and cannot be used</li> <li>Cancel</li> </ul> If you selected PKCS #11 Token, you will see <ul style="list-style-type: none"> <li>PKCS #11 Login (SSL client authentication)</li> <li>Cancel</li> </ul> |

## Logging into the Console



While logging into a Manager that has been configured to use Password-based or SSL Client Based authentication, if you try to log in using a certificate and the login fails, all subsequent attempts to use the username/password login will also fail during the same session. To work around this, restart the Console.

To start the Console, click **Login**. When you start the Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the Manager's certificate. The prompt will show details specific to your settings (following is just an example). Click **OK** to trust the Manager's certificate. The certificate will be permanently stored in the Console's truststore and you will not see the prompt again the next time you log in.



## Reconnecting to the ArcSight Manager

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

Connections to the ArcSight Manager cannot be re-established while the ArcSight Manager is restarting or if the Manager refuses the connection. In addition, you may see connection exceptions during the Retry process while the connection is lost or ArcSight Manager is restarting.

## Reconfiguring the ArcSight Console

You can reconfigure ArcSight Console at any time by running the following command within a command window from the Console's `bin` directory:

On Windows: `arcsight.bat consolesetup`

On Linux: `./arcsight consolesetup`

and follow the prompts.

## Uninstalling the ArcSight Console

Before uninstalling the ArcSight Console, exit the current session.

To uninstall on Windows, run the **Start->All Programs (Programs in the case of Windows XP)->ArcSight ESM Console ->Uninstall ArcSight ESM Console 6.0c**

program. If a shortcut to the Console was not installed on the Start menu, locate the Console's `UninstallerData` folder and run:

`Uninstall_ArcSight_ESM_Console.exe`

To uninstall on Unix hosts, open a command window on the `<ARCSIGHT_HOME>/UninstallerData` directory and run the command:

`./Uninstall_ArcSight_ESM_Console`



**Note**

The UninstallerData directory contains a file `.com.zerog.registry.xml` with Read, Write, and Execute permissions for everyone. On Windows hosts, these permissions are required for the uninstaller to work. However, on UNIX hosts, you can change the permissions to Read and Write for everyone (that is, 666).





## Chapter 4

# Using SmartConnectors

---

This chapter covers the following topics:

[“Installing the SmartConnector” on page 49](#)

[“Importing the Manager’s Certificate” on page 49](#)

SmartConnectors process raw data generated by various vendor devices throughout an enterprise. Devices are hardware and software products such as routers, anti-virus products, firewalls, intrusion detection systems (IDS), VPN systems, anti-DoS appliances, operating system logs, and other sources that detect and report security or audit information.

ArcSight SmartConnectors collect a vast amount of varying, heterogeneous information. Due to this variety of information, SmartConnectors format each event into a consistent, normalized ArcSight events, letting you find, sort, compare, and analyze all events using the same event fields. The “normalized” events are then sent to the ArcSight Manager and are stored in the database.

## Installing the SmartConnector

Installing and configuring the SmartConnector is a three step process:

- 1 Install the SmartConnector.

For an overview of the SmartConnector installation and configuration process, see the *SmartConnector User’s Guide*.

- 2 Import the Manager’s certificate to the Connector’s truststore. See the section [Importing the Manager’s Certificate](#) for details on how to do this.

- 3 Configure the SmartConnector.

For complete configuration instructions for a particular SmartConnector, see the configuration guide for that connector. The product-specific configuration guide provides specific device configuration information, installation parameters, and device event mappings.

## Importing the Manager’s Certificate

When setting up the connector for a primary destination, you will be prompted to import the Manager’s certificate. If you select **Import the certificate to the connector from destination** the Manager’s certificate will be imported automatically. If you choose not to do so, you must import the Manager’s certificate manually.

You will need to import the Manager's certificate manually for any additional destinations that you set up and also if installing the connector in FIPS with Suite B mode.

## Using keytoolgui to Import Manager's Certificate



If you have the agentsetup wizard running, be sure to close it before importing the Manager's certificate.

You will need to export the Manager's certificate before you can import it on the Smart Connector in the Smart Connector server.

You can do so by running the keytool utility or by using the keytoolgui as described below. For more information on the keytool utility, refer to the "Configuration" chapter in the *Administrator's Guide*.

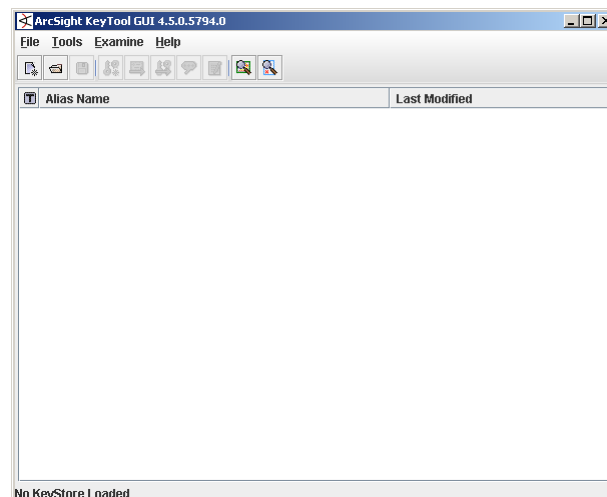
## Exporting the Manager's Certificate

To export the Manager's certificate:

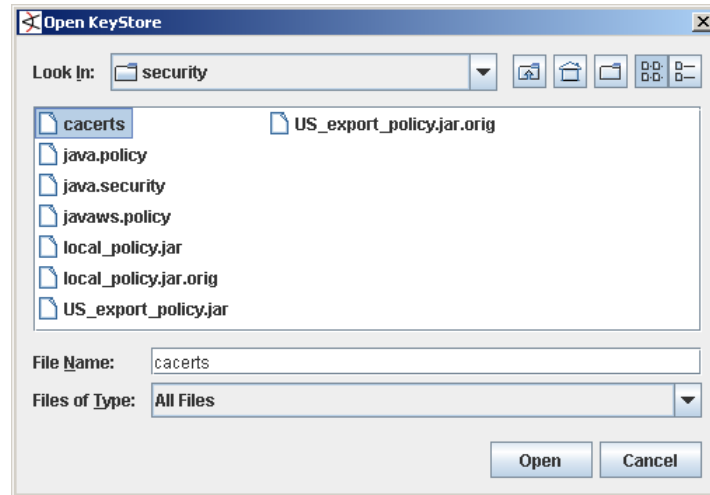
- 1 Open a shell window.
- 2 Run the following command from the Manager's `/opt/arcsight/manager/bin` directory while logged in as user "arcsight":

```
./arcsight keytoolgui
```

The keytoolgui interface will open.



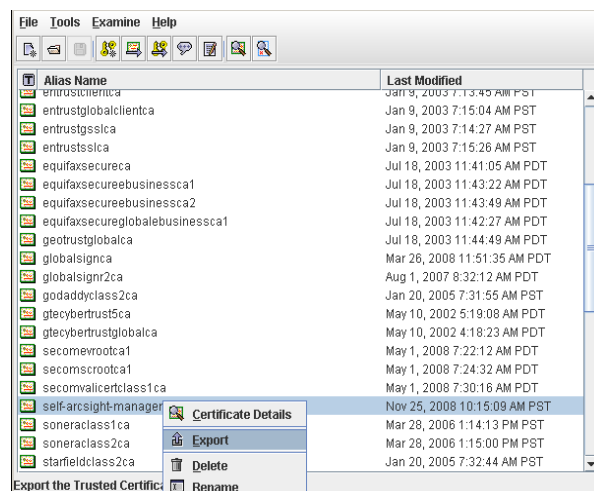
- 3 Select **File->Open KeyStore** from the menu and navigate to the Manager's truststore (**cacerts**) located in `/opt/arcsight/manager/jre/lib/security/` directory.



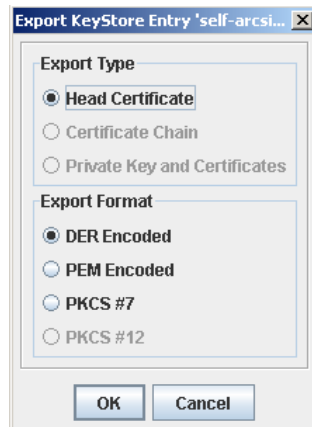
- 4 Enter the keystore password. The default password is "changeit" (without the quotes).



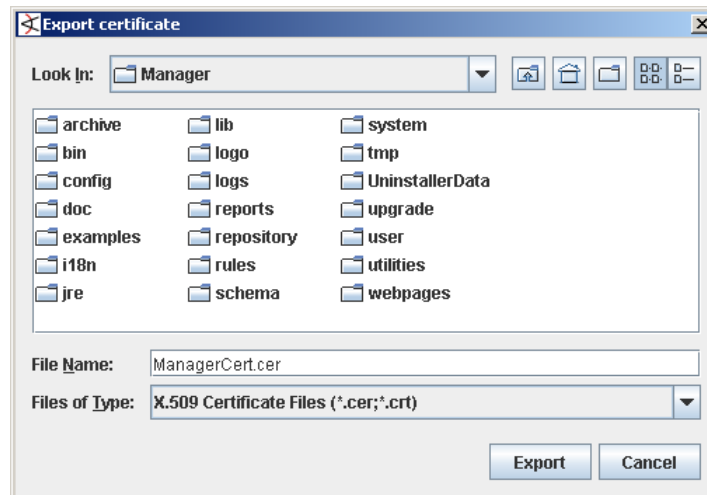
- 5 Right-click the Manager's certificate as shown below and select **Export**.



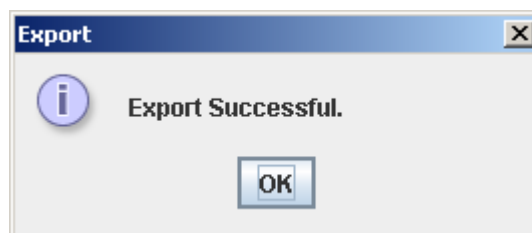
- 6 Accept the default settings in the following dialog and click **OK**.



- 7 Navigate to the location where you want to export the certificate and enter a file name in the File Name text box when naming the certificate and click **Export**.



- 8 You will see the following prompt when the certificate is exported successfully.



- 9 Click **OK** and exit the `keytoolgui`.
- 10 Transfer (or scp) this exported certificate file from the Manager machine to the Smart Connector server where you will be importing it into the SmartConnector.

## Importing the Manager's Certificate into the SmartConnector's Truststore

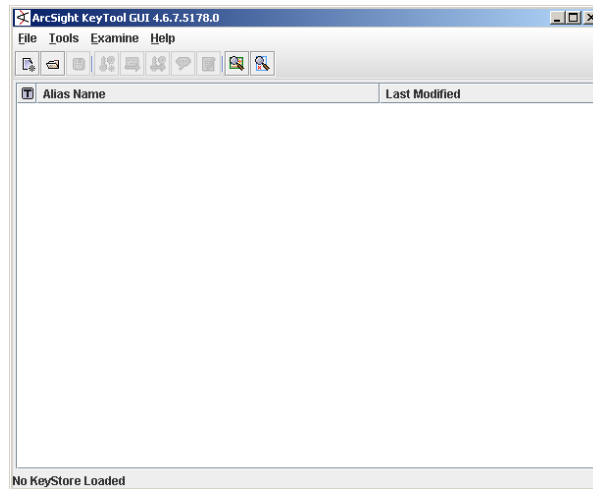
Import the certificate you exported above into the Connector's truststore.

To do so:

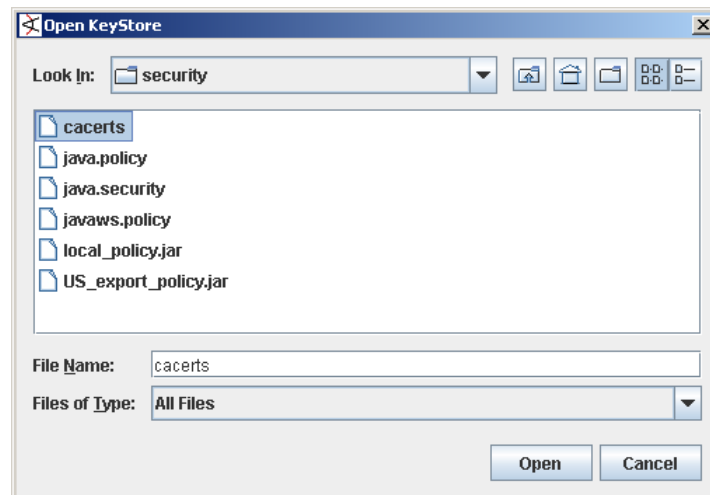
- 1 Open a shell window on the SmartConnector server.
- 2 While logged in as user "arcsight", run the following command from the Connector's `bin` directory (`/home/arcsight/ArcSightSmartConnectors/current/bin` on Unix and `C:\arcsight\ArcSightSmartConnectors\current\bin` on Windows):

```
./arcsight agent keytoolgui
```

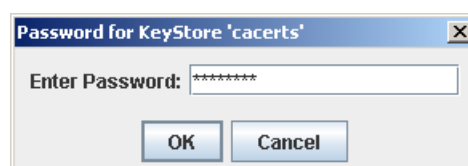
The keytoolgui interface will open.

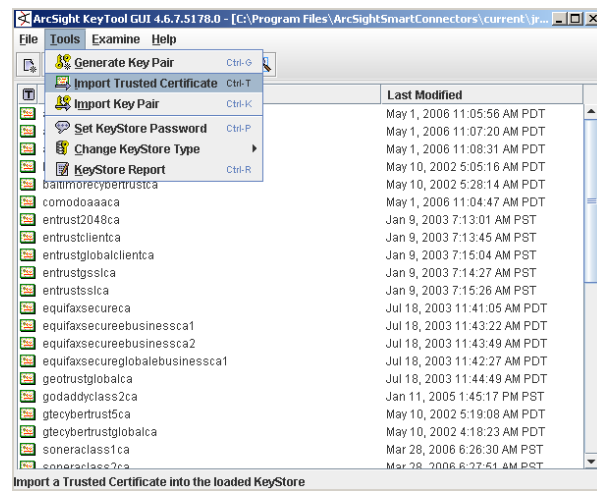
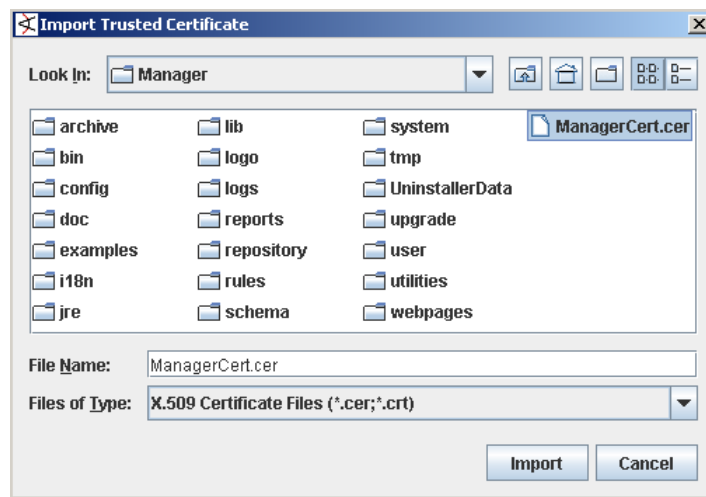
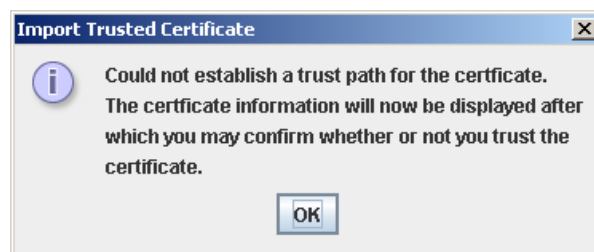


- 3 Select **File->Open KeyStore** from the menu and navigate to the Connector's truststore (`cacerts`) located in `/home/arcsight/ArcSightSmartConnectors/current/jre/lib/security` directory on Unix and `C:\arcsight\ArcSightSmartConnectors\current\jre\lib\security` on Windows.



- 4 Enter the password. The default password is "changeit" (without the quotes).



5 Click **Tools->Import Trusted Certificate**.6 Navigate to the Manager's certificate, select it and click **Import**.7 You will see the following prompt. Click **OK** to see the certificate details.

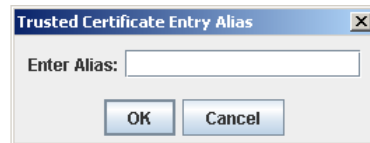
The **Certificate Details** dialog will be displayed.

8 Click **OK** on the **Certificate Details** dialog to accept the certificate.

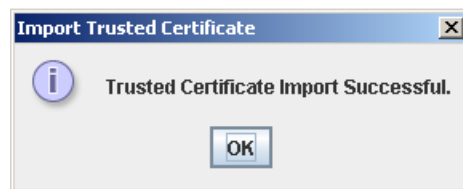
- 9 Click **Yes** in the following dialog.



- 10 Enter an alias for the certificate and click **OK**.



- 11 You will see the following message when the import is successful.



- 12 Click **OK**.

- 13 Click **File->Save KeyStore** to save the certificate in the Connector's truststore and exit the `keytoolgui` interface.

- 14 Run the following from the connector's `bin` directory:

```
./runagentsetup
```

and follow the directions in the wizard screens. Refer to the *SmartConnector User's Guide* for details on the wizard screens.





## Appendix A

# Troubleshooting

---

The following information may help solve problems that might occur when installing or using ESM. In some cases, the solution can be found here or in other ESM documentation, but HP ArcSight Customer Support is available if you need it.

This chapter covers the following topics:

["Location of Log files for Components" on page 57](#)  
["Customizing ESM Components Further" on page 59](#)  
["Fatal Error when Running the First Boot Wizard" on page 60](#)  
["Changing the IP Address of your machine" on page 61](#)  
["Changing the Host Name of the Machine After Running the First Boot Wizard" on page 62](#)

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

## Location of Log files for Components

The log files can be found in the following location:

| Log file name                               | location                                                                    | Description                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Suite Installer Logs</b>                 |                                                                             |                                                                                                                       |
| ArcSight_ESM_<version>_Suite_InstallLog.log | <a href="#">/opt/arcsight/suite</a><br>or<br><a href="#">/home/arcsight</a> |                                                                                                                       |
| <b>First Boot Wizard Logs</b>               |                                                                             |                                                                                                                       |
| fbwizard.log                                | <a href="#">/opt/arcsight/manager/logs/default/</a>                         | Contains detailed troubleshooting information logged during the steps in <a href="#">"Configuration" on page 21</a> . |

| Log file name                 | location                                                          | Description                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| firstbootsetup.log            | <a href="#">/opt/arcsight/manager/logs/</a>                       | Contains brief troubleshooting information about commands that ran during the steps in <a href="#">“Configuration” on page 21</a> . |
| <b>CORR-Engine Log Files</b>  |                                                                   |                                                                                                                                     |
| logger_server.log             | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Contains troubleshooting information about the CORR-Engine                                                                          |
| logger_server.out.log         | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | CORR-Engine stdout log file                                                                                                         |
| arcsight_logger.log           | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| logger_init_driver.log        | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| logger_init_setup.log         | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| logger_init.sh.log            | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| logger_wizard.log             | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| logger_wizard.out.log         | <a href="#">/opt/arcsight/logger/current/arcsight/logger/logs</a> | Logs for setting up the CORR-Engine                                                                                                 |
| <b>Manager Log Files</b>      |                                                                   |                                                                                                                                     |
| server.log                    | <a href="#">/opt/arcsight/manager/logs/default</a>                | Contains troubleshooting information about the Manager                                                                              |
| server.std.log                | <a href="#">/opt/arcsight/manager/logs/default</a>                | Contains the stdout output of the Manager                                                                                           |
| server.status.log             | <a href="#">/opt/arcsight/manager/logs/default</a>                | Contains a dump of all the MBeans, the memory status, thread status, etc.                                                           |
| <b>ArcSight Web Log Files</b> |                                                                   |                                                                                                                                     |
| webserver.log                 | <a href="#">/opt/arcsight/web/logs/default</a>                    | Contains troubleshooting information about ArcSight Web                                                                             |
| webserver.std.log             | <a href="#">/opt/arcsight/web/logs/default</a>                    | Contains the stdout output of ArcSight Web                                                                                          |
| server.status.log             | <a href="#">/opt/arcsight/web/logs/default</a>                    | Manager status monitoring log file                                                                                                  |

| Log file name                | location                                           | Description                                                                          |
|------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>Log file for services</b> |                                                    |                                                                                      |
| arcsight_services.log        | <a href="#">/opt/arcsight/services/logs/</a>       | Contains information from commands that manage ArcSight service processes.           |
| monit.log                    | <a href="#">/opt/arcsight/services/monit/data/</a> | Contains timing information from startup and shutdown of ArcSight service processes. |

## If you Encounter an Unsuccessful Installation

If you encounter an unsuccessful installation, or if your installation gets corrupted, do the following before reinstalling the product.

If your installation became corrupted after running `setup_services.sh`, run the following script as root user:

```
remove_services.sh
```

If your installation became corrupted before running `setup_services.sh`, perform the following steps as arcsight user:

- 1 Kill any ArcSight services that are currently running. Either:
  - a run `/opt/arcsight/services/init.d/arcsight_services killAllFast`
  - b Query if there are any arcsight processes running and manually kill them
- 2 Delete all arcsight-related files/directories under `/opt/arcsight` and `/tmp`
- 3 Delete any shortcuts created during installation (by default in the home directory of the "arcsight" user)

## Customizing ESM Components Further

The First Boot Wizard allows you to configure the ArcSight Manager and the CORR-Engine Storage. But, in the event that you would like to customize a component further, you can follow these instructions to start the setup program for the component:

### ArcSight Manager

While logged in as user *arcsight*,

- 1 Stop the Manager if it is running:
 

```
/sbin/service arcsight_services stop manager
```
- 2 Run the following command from `/opt/arcsight/manager/bin` directory:
 

```
./arcsight managersetup
```

- 3 Follow the prompts on the wizard screens. See the *Administrator's Guide* for information on any specific screen.
- 4 Restart the Manager after the wizard completes by running:  

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

## ArcSight Web

While logged in as user *arcsight*,

- 1 Stop ArcSight Web if it is running:  

```
/sbin/service arcsight_services stop arcsight_web
```
- 2 Run the following command from `/opt/arcsight/web/bin` directory:  

```
./arcsight webserversetup
```
- 3 Follow the prompts on the wizard screens. See the *Administrator's Guide* for information on any specific screen.
- 4 Start ArcSight Web after the wizard completes by running:  

```
/sbin/service arcsight_services start arcsight_web
```

## Fatal Error when Running the First Boot Wizard

If you encounter a fatal error while running the First Boot Wizard, the wizard will display an error message and then exit. Check the log files for the particular component for any error messages. The log files are listed in the section ["Location of Log files for Components" on page 57](#).

To resolve this issue, try the following steps:

- 1 Check the `/opt/arcsight/manager/logs/default/fbwizard.log` file to figure out where the error occurred.
- 2 Check to make sure that all the required TCP ports mentioned in the section ["Keep these TCP ports Open" on page 14](#) are open.
- 3 The First Boot Wizard can only be rerun if it did not reach the point where it configures the Manager. See section ["Rerunning the Wizard" on page 28](#) for more details on this. If your error occurred before any component got configured, restart the First Boot Wizard by running the following command from the `/opt/arcsight/manager/bin` directory when logged in as user "arcsight":

In GUI mode:

```
./arcsight firstbootsetup -boxster -soft
```

In console mode:

```
./arcsight firstbootsetup -boxster -soft -i console
```

## Changing the IP Address of your machine

In case you want to change the IP address of your machine after running the First Boot Wizard successfully, follow these steps:



Please note, that the Manager setup command must be run when logged in as user "arcsight."

- 1 Stop all ArcSight services by running (as user *arcsight*):  

```
/sbin/service arcsight_services stop all
```
- 2 Change the IP address of your machine.
- 3 Reboot the machine.
- 4 While logged in as user **arcsight**, run the following to start the setup program for the Manager from `/opt/arcsight/manager/bin` directory:  

```
./arcsight managersetup
```

This will open the Manager's setup wizard.

  - a Enter the new IP address (that you set for your machine in [Step 2](#) above) in the Manager Host Name field when prompted by the wizard.
  - b Make sure to select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new IP address.
- 5 Start the Manager by running (as user *arcsight*):  

```
/sbin/service arcsight_services start manager
```
- 6 Export the Manager's newly generated self-signed certificate and import it into ArcSight Web using the `keytoolgui` tool. See the *Administrator's Guide* for details on how to export and import a certificate. See the "Using Keytoolgui to Export a Certificate" and "Using Keytoolgui to Import a Certificate" sections in the "Configuration" chapter in the *Administrator's Guide* available on the HP ArcSight Customer Support download site for details on how to do this.
- 7 While logged in as user **arcsight**, run the following to start the setup program for ArcSight Web from the `/opt/arcsight/web/bin` directory:  

```
./arcsight websetup
```

  - a Enter the new IP address (that you set for your machine in [Step 2](#) above) in Webserver Host Name field when prompted.
  - b Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new IP address.
- 8 Start ArcSight Web by running (as user *arcsight*):  

```
/sbin/service arcsight_services start arcsight_web
```
- 9 Import the Manager's newly generated certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the `keytoolgui`. See the "Using Keytoolgui to Import a Certificate" section in the "Configuration"

chapter in the *Administrator's Guide* available on the HP ArcSight Customer Support download site for details on how to do this.

- 10 Test to make sure that the clients can connect to the Manager.

## Changing the Host Name of the Machine After Running the First Boot Wizard



Please note that the Manager setup command must be run when logged in as user "arcsight."

In case you want to change the host name of the machine after running the First Boot Wizard successfully, follow these steps:

- 1 Stop all services by running (as user *arcsight*):

```
/sbin/service arcsight_services stop all
```

- 2 Change the host name of your machine.

- 3 Reboot the machine.

If you had entered a host name (instead of an IP address) when configuring the Manager in the First Boot Wizard, then you will be required to do the following in addition to the steps mentioned above:

- 4 Stop the Manager by running (as user *arcsight*):

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

- 5 Stop ArcSight Web by running (as user *arcsight*):

```
/sbin/service arcsight_services stop arcsight_web
```

- 6 While logged in as user **arcsight**, run the Manager's setup program from the `/opt/arcsight/manager/bin` directory as user "arcsight":

```
./arcsight managersetup
```

- a Enter the new host name (that you set for your machine in the steps above), in the Manager Host Name field when prompted by the wizard.

- b Make sure to select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new host name.

- 7 Start the Manager by running (as user *arcsight*):

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

- 8 Export the Manager's newly generated self-signed certificate and import it into ArcSight Web using the `keytoolgui` tool. See the "Using Keytoolgui to Export a Certificate" and "Using Keytoolgui to Import a Certificate" sections in the "Configuration" chapter in the *Administrator's Guide* available on the HP ArcSight Customer Support download site for details on how to do this.

- 9 While logged in as user *arcsight*, run the following to start the setup program for ArcSight Web from the `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

- a** Enter the new host name in Webserver Host Name field when prompted.
- b** Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new hostname.

- 10** Start ArcSight Web by running (as user *arcsight*):

```
/sbin/service arcsight_services start arcsight_web
```

- 11** Import the Manager's certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the keytoolgui. See the "Using Keytoolgui to Import a Certificate" section in the "Configuration" chapter in the *Administrator's Guide* available on the HP ArcSight Customer Support download site for details on how to do this.
- 12** Test to make sure that the clients can connect to the Manager.





# Default Settings for Components

This appendix gives you the default settings for each software component in ESM. It covers the default settings for the following:

[“General” on page 65](#)

[“CORR-Engine” on page 65](#)

[“ArcSight Manager” on page 66](#)

[“ArcSight Web” on page 67](#)

You can always customize any component by running its setup program.

The following tables list the default settings for each component.

## General

| Setting                         | Default Value            |
|---------------------------------|--------------------------|
| default password for truststore | <a href="#">changeit</a> |
| default password for cacerts    | <a href="#">changeit</a> |
| default password for keystore   | <a href="#">password</a> |

## CORR-Engine

The following are some of the default values that have been pre-configured in the CORR-Engine for you:

| Setting            | Default Value                        |
|--------------------|--------------------------------------|
| Location of Logger | <a href="#">/opt/arcsight/logger</a> |
| Database user name | <a href="#">arcsight</a>             |
| Database Port      | <a href="#">3306</a>                 |

## ArcSight Manager



ArcSight Manager uses a self-signed certificate, which gets generated for you when you configure the system using the First Boot Wizard. When you log into the Console for the very first time you will be prompted to accept the Manager's certificate. You can either click Yes in that dialog or optionally import the Manager's certificate manually at a later time.

The following are some of the default values that have been pre-configured in ArcSight Manager for you:

| Setting                                                              | Default Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location of Manager                                                  | <code>/opt/arcsight/manager</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Manager host name                                                    | Host name or IP address of ESM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Manager Port                                                         | <code>8443</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Manager license file                                                 | Please obtain from Customer Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Java Heap Memory                                                     | 8 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Authentication Type                                                  | Password Based                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Type of certificate used                                             | self-signed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Default password for keystore                                        | <code>password</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Default password for cacerts                                         | <code>changeit</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Default password for truststore                                      | <code>changeit</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Default password for nssdb and nssdb.client (both used in FIPS mode) | <code>changeit</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| E-mail Notification                                                  | <p>Internal SMTP server. If you want to use an External SMTP server,</p> <ol style="list-style-type: none"> <li>1 Stop the Manager by running the following command (as user <i>arcsight</i>):<br/> <code>/sbin/service arcsight_services stop manager</code></li> <li>2 Run the following command from the <code>/opt/arcsight/manager/bin</code> directory and set up the external SMTP server when prompted:<br/> <code>./arcsight managersetup</code></li> <li>3 Start the Manager by running (as user <i>arcsight</i>):<br/> <code>/sbin/service arcsight_services start manager</code></li> </ol> |
| Sensor Asset Auto Creation                                           | Enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Packages/default content installed                                   | All system content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## ArcSight Web

The following are some of the default values that have been pre-configured in ArcSight Web for you.

| Setting                         | Default Value                     |
|---------------------------------|-----------------------------------|
| Location of ArcSight Web        | <a href="#">/opt/arcsight/web</a> |
| ArcSight Web host name          | Host name or IP address of ESM    |
| ArcSight Web Port               | <a href="#">9443</a>              |
| Java Heap Memory                | 1 GB                              |
| Authentication Type             | Password Based                    |
| Type of certificate used        | self-signed                       |
| Default password for keystore   | <a href="#">password</a>          |
| Default password for cacerts    | <a href="#">changeit</a>          |
| Default password for truststore | <a href="#">changeit</a>          |
| Default password for nssdb      | <a href="#">changeit</a>          |



## Appendix C

# Using the PKCS#11 Token

---

This appendix covers the following topics:

- ["What is PKCS?" on page 69](#)
- ["PKCS#11 Token Support in ESM" on page 70](#)
- ["References to <ARCSIGHT\\_HOME>" on page 70](#)
- ["Setting Up to Use a CAC Card" on page 70](#)
- ["Logging in to the Management Console Using CAC" on page 79](#)
- ["Using CAC with ArcSight Web" on page 80](#)

ESM supports the use of a PKCS#11 token, such as the Common Access Card (CAC), which is used for identity verification and access control. The PKCS#11 token authentication works using the SSL client-side authentication.

PKCS#11 authentication is not supported with Radius, LDAP and Active Directory authentication methods.

## What is PKCS?

Public Key Cryptography Standards (PKCS), published by RSA Laboratories, comprises a group of standards used for reliable and secure public key cryptography. Public Key Cryptography works by encrypting the data at the sender's end and decrypting it at the receiver's end.

## PKCS#11

PKCS#11, one of the PKCS standards, is an API defining a generic interface to cryptographic tokens, software tokens and hardware tokens such as hardware security modules and smartcards. A cryptographic token is a security device that is used to authorize the use of the software or hardware, such as the smartcard or Common Access Card (CAC). The credentials of the authorized user are stored on the hardware itself. ESM uses the PKCS#11 interface provided by the Network Security Services (NSS) cryptographic module to communicate with it (the NSS cryptographic module). The use of PKCS #11 is an example of client-side authentication.

## PKCS#12

PKCS#12, also a PKCS standard, defines a file format, the .pfx file format, which is used to store private keys and their accompanying public key in a single encrypted file in the NSS DB. The .pfx files are password protected. Key pairs stored in NSS DB are required to be

stored in this format. When ArcSight Web and Manager are configured to run in FIPS mode, their key pairs are stored in the .pfx format in their NSS DB. PKCS #12 is applicable to server-side authentication.

## PKCS#11 Token Support in ESM

ESM supports any PKCS#11 Token vendor that supports PKCS#11 2.0 or above. You have to make sure that The vendor's driver and the PKCS#11 driver DLL are installed on the machine on which you plan to use the PKCS#11 token.

Before you use the PKCS#11 token, make sure that you have installed the provider software on the ArcSight Console system with which you plan to use the PKCS#11 token. Refer to your PKCS#11 token provider's documentation on how to install and configure your cryptographic device.

You can use a PKCS#11 token regardless of the mode in which the client is running (FIPS 140-2 mode or default mode). However you must use "Password or SSL Authentication," which you set up as follows:

- 1 Log in to the Management Console.
- 2 Go to the **Administration** tab.
- 3 Select **Configuration Management**, on the left.
- 4 Select **Authentication Configuration**.
- 5 Select **Password or SSL Client Based** authentication.
- 6 Restart the Manager.

To use a PKCS #11 token, make sure that the token's CA's root certificate and the certificate itself are imported into the Manager's truststore. You also have to map the CAC card's Common Name (CN) to the External User ID in the ArcSight Console. In the Management Console, you can edit the External ID to match the common name on the Admin tab.

## References to <ARCSIGHT\_HOME>

<ARCSIGHT\_HOME> in the paths represents

- `/opt/arcsight/manager` for the Manager,
- `/opt/arcsight/web` for ArcSight Web.
- Whatever path you specified when you installed the ArcSight Console

## Setting Up to Use a CAC Card

Even though ESM supports authentication through any PKCS#11 token, this appendix, covers how to use the ActivClient's Common Access Card (CAC) as an example.

### Install the CAC Provider's Software

Before you use the Common Access Card (CAC), make sure that you have installed its software on each client system. That includes the ArcSight Console and any machine with a

browser from which you intend to access the Management Console. Refer to your CAC provider's documentation on how to install and configure it.



Note

Install both the 32-bit version and the 64-bit version of the ActivClient software if you are on a 64-bit system. You can do so by double-clicking on the [setup.exe](#) link instead of the [.msi](#) files for the specific platform.

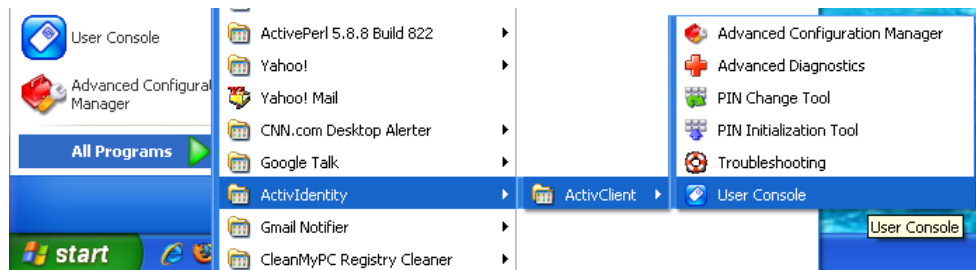
## Map a User's External ID to the CAC's Subject CN

The CAC card contains three types of certificate, Signature, Encryption and ID certificates. Only ID certificate is supported.

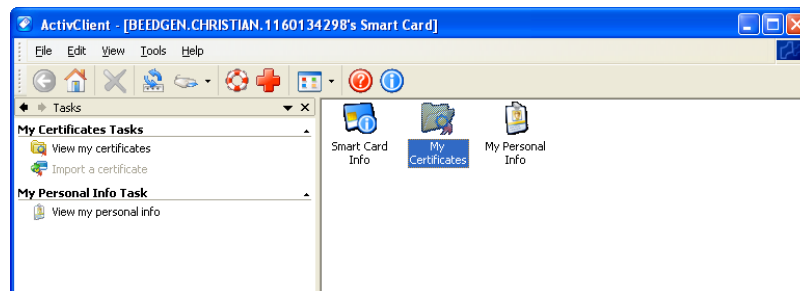
Map the Common Name (CN) on the CAC to a User's External ID on the Manager. The external user ID must be identical to the Common Name that appears in the CAC card's ID certificate (include any spaces and periods that appear in the Common name). This allows the Manager to know which of its user is being represented by the identity stored in the CAC card.

You can do this in the Management Console's **Admin** tab under User Management, when adding or editing a user.

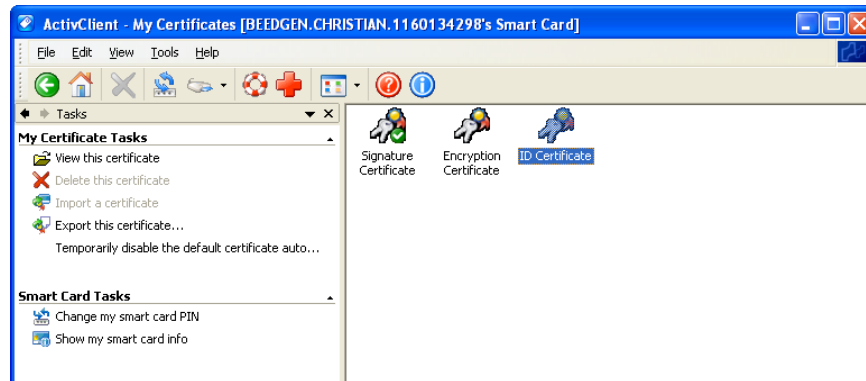
- 1 Obtain the Subject CN from the CAC card.
  - a Insert the CAC card into the reader if not already inserted.
  - b Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



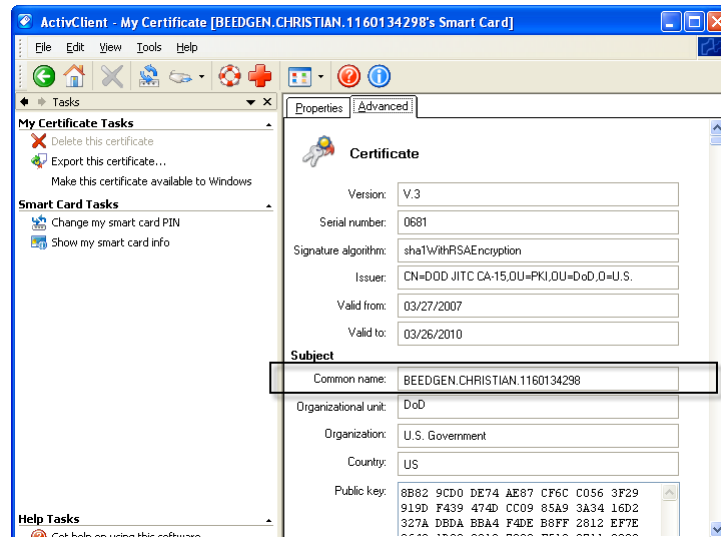
- c Double-click **My Certificates** in the following screen:



- d Double click **ID Certificate** in the following screen:



- e Click on the **Advanced** tab and copy the contents in the Common name text box. You will have to copy it by hand on to a sheet of paper. Using the context menu to copy is not supported.



- 2 In the Management Console, go to the **Administration** tab to edit the user to make the external ID match the CN.
  - a Select **User Management**, on the left.
  - b In the hierarchy tree on the left, click on the group containing the user.
  - c To edit a user, click anywhere on the user's row in the list. The user details fields appear in the lower half of the list.
  - d In the External ID field, enter the CN you obtained in step 1 and click **Save**. It must be identical, character by character.

Alternately, you can make the external ID match the CN in the ArcSight Console:

- a In the ArcSight Console, go to **Resources > Users** and double-click the user whose External ID you want to map to the CAC card common name. This will open the Inspect/Edit pane for that user.
- b Enter the CN you obtained in step 1 into the **External User ID** field and click **Apply**.



## Obtain the CAC's Issuers' Certificate

PKCS#11 Token authentication is based on SSL client-side authentication. In the case of the Common Access Card, the key pair for the client (the CAC device) is stored within the card itself. You need to export the CAC's certificate from its keystore so that you can extract the root CA and any intermediate certificates from this certificate.

If your certificate is issued by an intermediate CA, export not only the issuer (the intermediate root CA) certificate, but also, its top root CA certificate.

### Option 1:

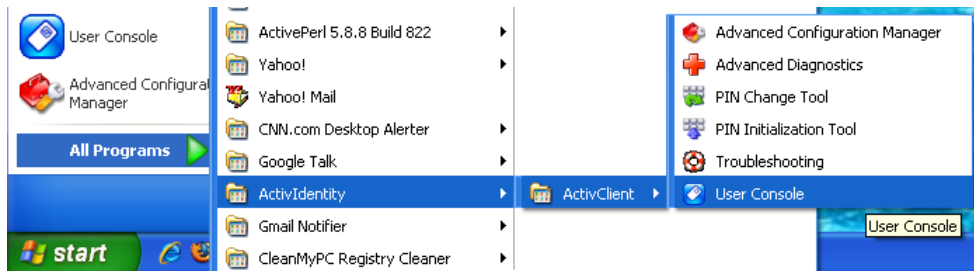
You can obtain the CAC card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

### Option 2:

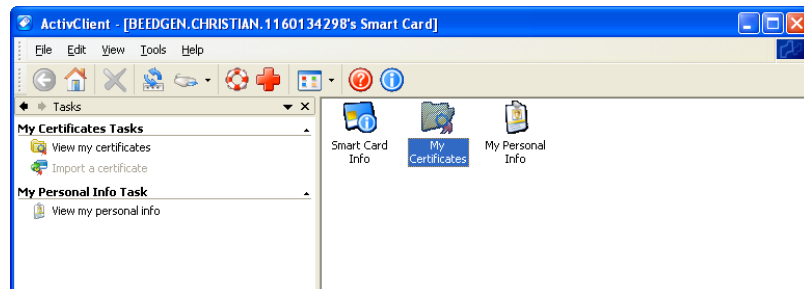
You can export the CAC card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

The steps to extract the CAC card's certificate from the card are:

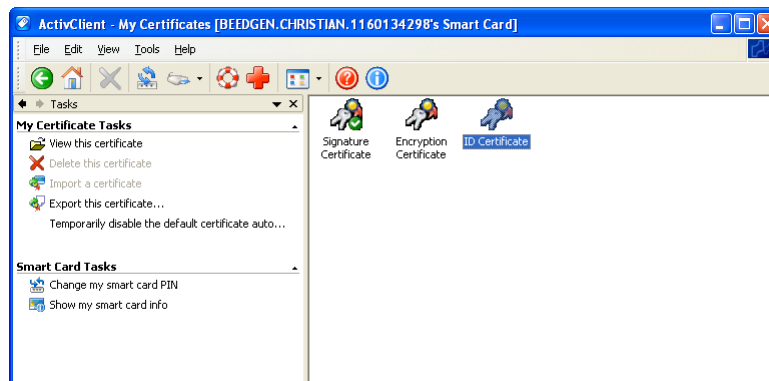
- 1 Insert the CAC card into the reader if not already inserted.
- 2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



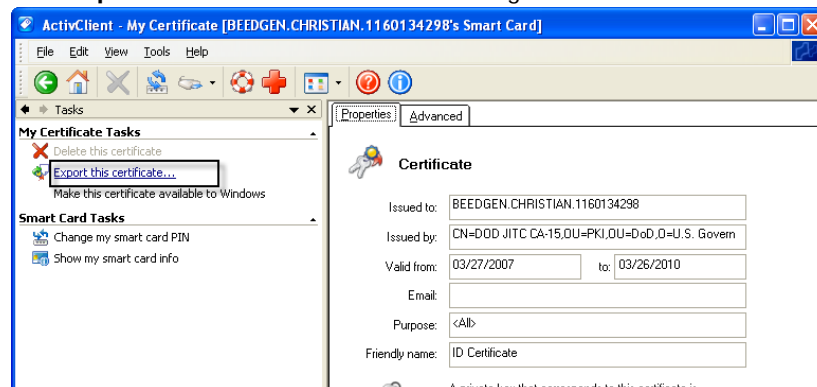
- 3 Double click **My Certificates** in the following screen:



- 4 Double click **ID Certificate** in the following screen:



- 5 Click **Export this certificate...** in the following screen:



- 6 Enter a name for the certificate in the **File name** box and navigate to a location on your machine where you want to export it to and click **Save**.
- 7 When you see the success message, click OK.
- 8 Exit the ActivClient window.

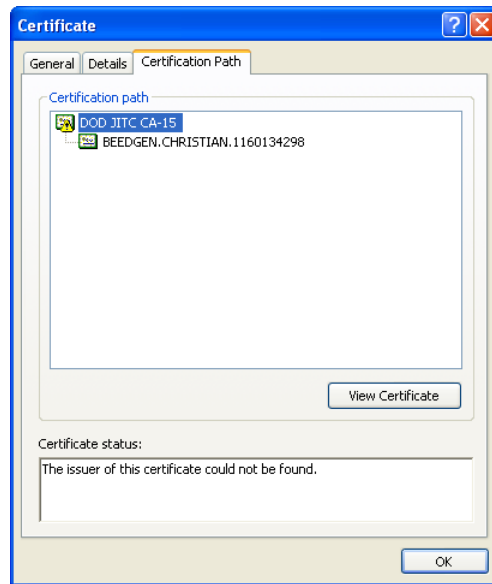
## Extract the Root CA Certificate From the CAC Certificate

The CAC certificate signer's CA root certificate and any intermediate signers' certificate(s) have to be imported into the Manager's `nssdb` (in FIPS mode) or `truststore` (in default mode).

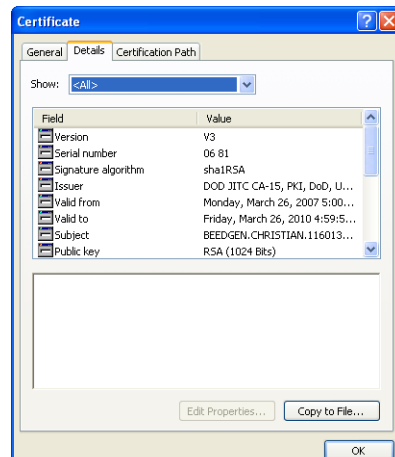
You should extract all intermediate certificates too (if any exist) using the following steps:

- 1 Double-click the CAC's certificate that you exported. The Certificate interface will open.

- 2 Click the **Certification Path** tab and select the root certificate as shown in the example below:



- 3 Click **View Certificate**.
- 4 Click the **Details** tab and click **Copy to File...**



- 5 The Certificate Export Wizard opens. Follow the prompts in the wizard screens and accept all the defaults.
- 6 Enter a name for the CAC root CA certificate file when prompted and continue with the wizard by accepting all the defaults. The certificate is exported to the same location as the CAC certificate from which you extracted it.
- 7 Exit the Certificate dialog.

## Import the CAC Root CA Certificate into the Manager

This procedure is slightly different depending on whether you are in FIPS or default mode:

### FIPS Mode - Import into the ESM Manager's nssdb

To import the certificate into the Manager's nssdb:

- 1 Stop the Manager as user *arcsight*, if it is running:

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

- 2 Import the CAC card signer's CA root certificate by running:

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



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

- 3 Restart the Manager as user *arcsight* by running:

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

### Default Mode - Import into the Manager's Truststore

Use the following procedure to import the CAC card's root CA certificate into the Manager's truststore:

- 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 `/bin` directory.  

```
./arcsight keytoolgui
```
- 2 Click **File->Open keystore** and navigate to the truststore (`/opt/arcsight/manager/config/jetty/truststore`) of the component.
- 3 Select the store named `truststore` and click **Open**.
- 4 Enter the password for the truststore when prompted. The default password is 'changeit' (without quotes).
- 5 Click **Tools->Import Trusted Certificate** and navigate to the location of the certificate that you want to import.
- 6 Click **Import**.
- 7 When you see the message that the certificate information will be displayed, click **OK**.
- 8 The Certificate details are displayed. Click **OK**.
- 9 When asked if you want to accept the certificate as trusted, click **Yes**.
- 10 Enter an alias for the Trusted Certificate you just imported and click **OK**.
- 11 When you see the message that the import was successful, click **OK**.
- 12 Save the truststore file.

- 13** Restart the Manager as user *arcsight* by running:

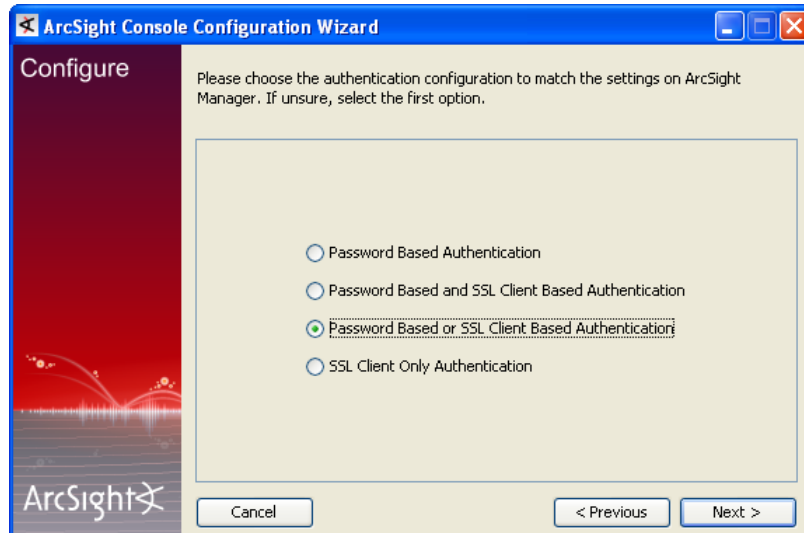
```
/sbin/service arcsight_services start manager
```

## Select Authentication Option in Console Setup

The authentication option on the Console should match the authentication option that you set on the Manager. Run the Console setup program and either confirm or change the authentication on the Console to match that of the Manager. To do so:

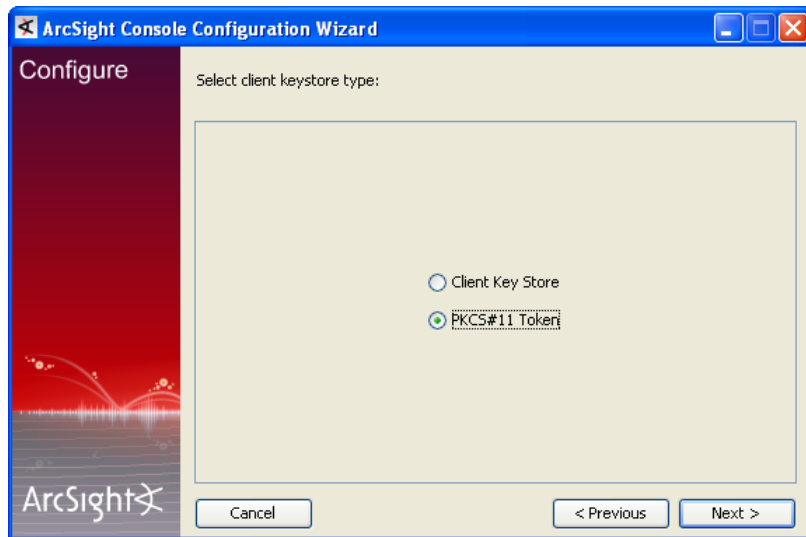
- 1** Stop the Console if it is running.
- 2** Run the Console's setup program from the Console's `bin` directory:  

```
./arcsight consolesetup
```
- 3** Follow the prompts in the wizard screens by accepting all the defaults until you get to the screen for the authentication option shown in the next step.
- 4** Select the authentication that you selected for the Manager in the following screen.



- 5** Follow the prompts in the next few screens by accepting the defaults.

- 6 Select **PKCS #11 Token** option in the following screen.



- 7 Enter the path or browse to the PKCS #11 library when prompted.

If you are using a vendor other than ActivClient, this should point to the library location for that installation.

If you are using ActiveClient, by default the PKCS #11 library is located in:

On 32-bit Windows:

`C:\Program Files\ActivIdentity\ActivClient\acpkcs211.dll`

On 64-bit Windows:

`C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`  
(this is the 32-bit version of the ActivClient library)

- 8 Complete the setup program by accepting all the defaults.
- 9 Restart any running ArcSight Consoles.

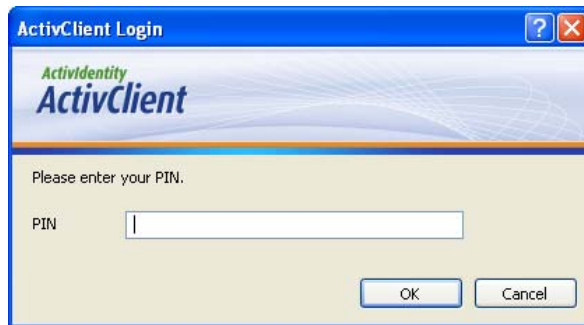
## Logging in to the Console Using CAC

When you start the Console, you will see a screen with a PKCS #11 login button.

You have the option to log in using one of the following methods:

- Username and password combination (For this option, disconnect the CAC card.)
- PKCS#11 Login

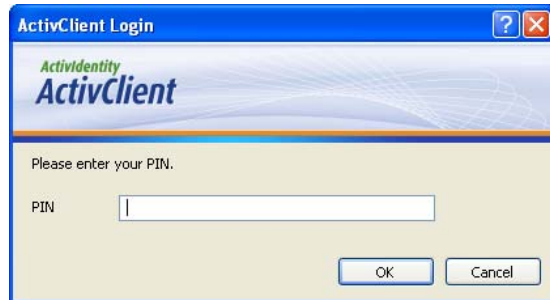
To log in using CAC, select the PKCS #11 Login option. In the following dialog, enter the PIN number of your ActivClient card in the **PIN** text box.



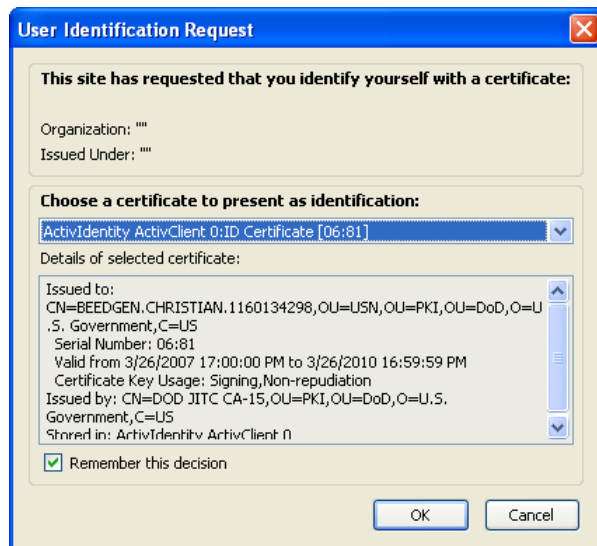
## Logging in to the Management Console Using CAC

Use a supported web browser such as Firefox or Internet Explorer to connect to the Management Console.

- 1 Make sure that the CAC card is securely placed in its card reader.
- 2 Go to URL <https://<hostname>:8443/>.
- 3 You will be requested to enter your PIN



If using Firefox, you will see an exception. Click 'Add exception', then generate and confirm the certificate key. You will see the following dialog. Click **OK**.



- 4 At the Management Console login, *do not* enter any user ID or password. Leave them both blank and click **Login**.

## Using CAC with ArcSight Web

You access ArcSight Web from the Management Console. When the Management Console is set up for CAC, no additional setup is required to access ArcSight Web, because its CAC access is handled by the Management Console.



## Appendix D

# ESM in FIPS Mode

---

This section covers the following topics:

- [“What is FIPS?” on page 81](#)
- [“Network Security Services Database \(NSS DB\)” on page 82](#)
- [“What is Suite B?” on page 82](#)
- [“NSS Tools Used to Configure Components in FIPS Mode” on page 83](#)
- [“TLS Configuration in a Nutshell” on page 83](#)
- [“Using PKCS #11 Token With a FIPS Mode Setup” on page 85](#)
- [“Installing ArcSight Console in FIPS Mode” on page 85](#)
- [“Configure Your Browser for FIPS” on page 90](#)
- [“Installing SmartConnectors in FIPS mode” on page 91](#)
- [“How do I Know If My Installation is FIPS Enabled?” on page 91](#)

ESM supports the Federal Information Processing Standard 140-2 (FIPS 140-2) and Suite B. You can choose to install the product components in FIPS mode if you have the requirement to do so.



- When the Manager is installed in FIPS mode, all other components must also be installed in FIPS mode.

## What is FIPS?

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 a piece of hardware or a software or a combination of the two which is used to implement cryptographic logic. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet the FIPS 140-2 standard.



To be FIPS 140-2 compliant, you need to have all components configured in the FIPS 140-2 mode. Even though a Manager running in FIPS mode can accept connections from non-FIPS mode components, if you opt for such a mixed configuration, you will not be considered FIPS 140-2 compliant. ArcSight recommends that you run all components in FIPS mode in order to be fully FIPS 140-2 compliant.

Mozilla's Network Security Services (NSS) is an example of FIPS certified cryptographic module. It is the core and only cryptographic module used by ESM in FIPS mode. NSS is an open source security library and collection of security tools. It is FIPS 140-2 compliant and validated. The NSS cryptographic module provides a PKCS #11 interface for secure communication with ESM. You can configure NSS to use either an internal module or the FIPS module. The FIPS module includes a single built-in certificate database token, the [Network Security Services Database \(NSS DB\)](#), which handles both cryptographic operations and the communication with the certificate and key database files.

## Network Security Services Database (NSS DB)

A difference between default mode and FIPS mode is that in default mode you use the keystore and truststore to store key pairs and certificates respectively in JKS format, whereas in FIPS mode both key pairs and certificates are stored in NSS DB. Key pairs are stored in the .pfx format (in compliance with PKCS #12 standard) in NSS DB. The NSS DB is located in:

- `/opt/arcsight/manager/config/jetty/nssdb` on the Manager
- `<ARCSIGHT_HOME>/current/config/nssdb.client` on the ArcSight Console
- `/opt/arcsight/web/config/jetty/webnssdb` on ArcSight Web



The default password for the NSS DB on every component is "changeit" without the quotes. However, we recommend that you change this password by following the procedure in section "Changing the Password for NSS DB" in the *Administrator's Guide*.

---

## What is 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.



- Not all ESM versions support the FIPS with Suite B mode. Refer to the ESM Product Lifecycle Document available on the Protect 724 website for supported platforms for FIPS with Suite B mode.
  - When the ESM Manager is installed in FIPS with Suite B compliant mode, all components (ArcSight Web, ArcSight Console, SmartConnectors, and Logger, if applicable) must be installed in FIPS with Suite B compliant mode, and browser used to access ESM must be FIPS enabled.
  - Before installing ESM in FIPS with Suite B mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled Manager.
- 

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.

## NSS Tools Used to Configure Components in FIPS Mode

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 generate key pairs and import and export certificates.
- `runmodutil` - is the NSS module configuration tool. It is used to enable or disable the FIPS module and change Keystore passwords. 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`.
- `runpk12util` - is an import and export tool for PKCS #12 format key pairs (.pfx files).

See "Appendix A, Administrative Commands" in the *Administrator's Guide* for details on the above command line tools. You can also refer to the 'NSS Security Tools' page on the Mozilla website for more details on any of the above NSS tools (make sure to search for them as `certutil`, `modutil`, or `pk12util`).

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

```
arcsight <command_name> -H
```

## TLS Configuration in a Nutshell

TLS configuration involves either server side authentication only or both server side and client side authentication. Setting up client side authentication is optional. To configure ESM in FIPS mode, you need to set up TLS configuration on the Manager, Console, and ArcSight Web.

Since TLS is based on SSL 3.0, we recommend that you have a good understanding of how SSL works. Please read the section "Understanding SSL Authentication" in the *Administrator's Guide* for details on how SSL works.

TLS and SSL require the server to have a public/private key pair and a cryptographic certificate linking the server's identity to the public key. The certificate should be signed by an entity that the client trusts. The clients, in turn, should be configured to 'trust' this entity. If the server and clients are controlled by the same authority then certificates can be created locally (self-signed certificates). A more secure approach would be to get the certificate signed by an organization that clients are pre-configured to trust. This involves dealing with one of the many commercial Certification Authorities (CAs).

Refer to the Administrator's Guide for information on upgrading an existing default mode installation into FIPS mode.

## Understanding Server Side Authentication

The first step in an SSL handshake is when the server (Manager) authenticates itself to the client (Console, ArcSight Web). This is called server side authentication. To set up TLS configuration on your Manager for server side authentication, you need:

- A key pair in your Manager's NSS DB.

The Manager's certificate, which incorporates the public key from the key pair located in the Manager's NSS DB. By default this is a self-signed certificate. Next, you should export the Manager's certificate from its NSS DB and lastly import this certificate into the NSS DB of the clients that will be connecting to this Manager.

## Understanding Client Side Authentication

SSL 3.0 and TLS support client side authentication which you can optionally set up as an extra measure of security. Client side authentication consists of the client authenticating itself to the server. In an SSL handshake, client side authentication, if set up, takes place after the server (Manager) has authenticated itself to the client (Console or ArcSight Web). At this point, the server requests the client to authenticate itself.

For the Console to authenticate itself to the Manager, you should have the following in the Console's NSS DB:

- A key pair.
- The Console's certificate, which incorporates the Console's public key.

If you plan to use PKCS #11 token such as the Common Access Card, you will be required to import the token's certificate into the Manager's NSS DB as the token is a client to the Manager.

For detailed procedures on each of the steps mentioned above, refer to ["Setting up Client-Side Authentication" on page 172](#) in the *Administrator's Guide*.

## Setting up Authentication on ArcSight Web - A Special Case

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 but has to authenticate itself to web browsers.

To authenticate the Manager, it should have the Manager's certificate. That certificate is imported automatically during installation.

The web browsers that try to connect to ArcSight Web import ArcSight Web's certificate into their truststore and use it to trust the webserver.

## Exporting the Manager's certificate for Other Clients

You are required to have this exported certificate available when installing clients that connect to this Manager, such as Connectors. (ArcSight Console can skip this step, it automatically imports the certificate.) You have to import this certificate into the clients' NSS DB (For Connectors that is `<ARCSIGHT_HOME>/current/user/agent/nssdb.client`) when installing them. Importing the Manager's certificate allows the clients to trust the Manager.

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

```
./arcsight runcertutil -L -n mykey -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o <absolute_path_to
_Managercertificatename.cert>
```



The `-o` specifies the absolute path to the location where you want the exported Manager's certificate to be placed. If you do not specify the absolute path the file will be exported to the `/opt/arcsight/manager` directory by default.

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

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

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

## References to ARCSIGHT\_HOME

`<ARCSIGHT_HOME>` in the paths represents:

- `/opt/arcsight/manager` for the Manager
- `/opt/arcsight/web` for ArcSight Web
- Whatever path you specified when you installed the ArcSight Console

## Using PKCS #11 Token With a FIPS Mode Setup

If you plan to use a PKCS #11 Token, such as the ActivClient's Common Access Card (CAC), you need to follow the steps below.

For details on any of these steps, see [Appendix C, Using the PKCS#11 Token, on page 69](#).

- 1 Install the CAC provider's software on each client machine. That includes the ArcSight Console and every machine using a browser to access ArcSight Web or the Management Console. See ["Install the CAC Provider's Software" on page 70](#).
- 2 Export the CAC card's certificate from the card.
- 3 Extract the root CA's certificate from the CAC card's certificate.
- 4 Import the CAC card's certificate and root CA's certificate into the Manager's nssdb.

## Installing ArcSight Console in FIPS Mode



If you would like to set up client-side authentication on the Console, refer to the *Administrator's Guide* for detailed steps to do so.

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`.

Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager.

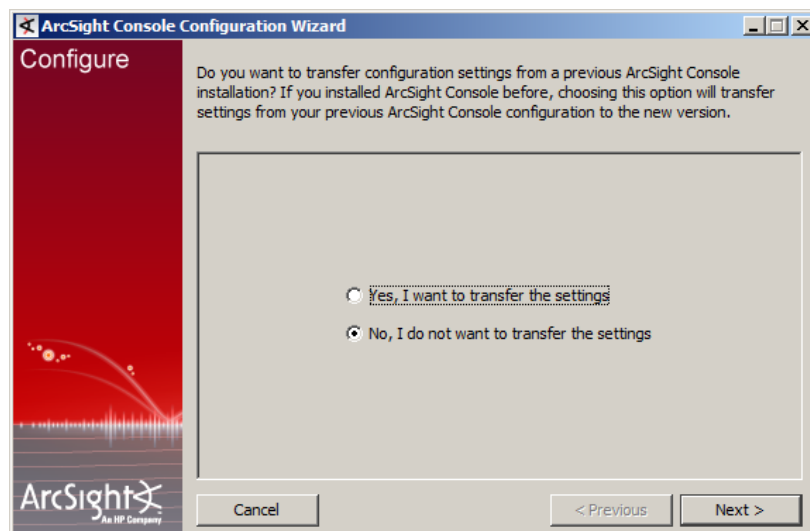
Refer to the ESM Product Lifecycle document available on the Protect 724 website (<https://protect724.arcsight.com>) for details on supported platforms for the Console.

This section tells you how to install the Console in FIPS mode only. For details on installing the Console in default mode, refer to the “Installing ArcSight Console” chapter, earlier in this guide.

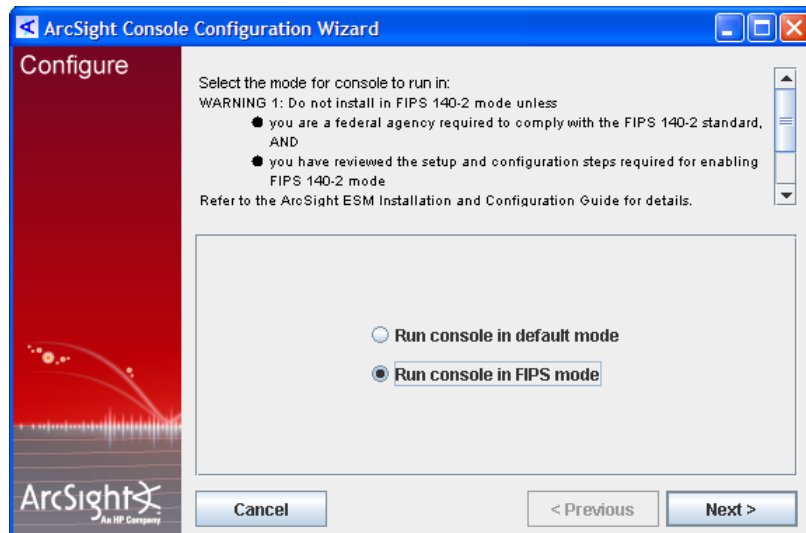
In order for an ArcSight Console to communicate with a FIPS enabled Manager, the Console must trust the Manager. This trust is established by importing the Manager's certificate into the Console's NSS DB (`<ARCSIGHT_HOME>/current/config/nssdb.client`). After you configure the ArcSight Console for FIPS, it will automatically import the Manager's certificate the first time you start it.

To install the Console in FIPS mode:

- 1 Run the self-extracting archive file that is appropriate for your target platform.
- 2 Follow the prompts in the wizard screens. Refer to “Installing ArcSight Console” chapter for details on each screen.
- 3 Select **No, I do not want to transfer the settings** in the following screen and click **Next**.



- 4 Next, you will see the following screen:



Select **Run console in FIPS mode** and click **Next**.

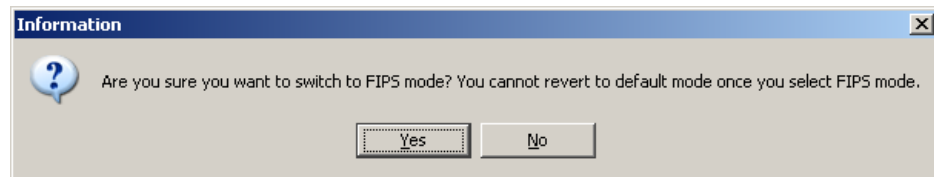


Note

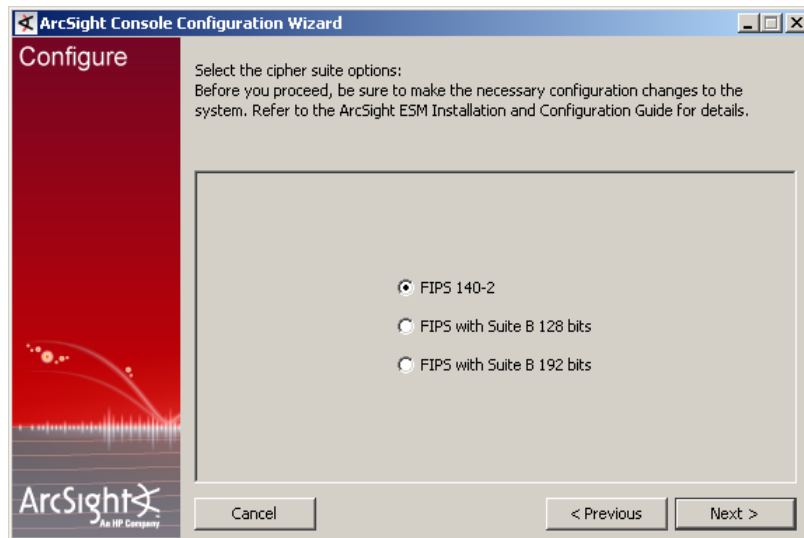
On the Windows XP, SP2 platform, you may see an error asking you to check the certificates in the NSSDB even though you have followed the steps to import the Manager's certificate into the NSSDB successfully. If you encounter this error:

- 1 Either delete or rename the `C:\Windows\system32\nspr4.dll` file.
- 2 Resume your Console installation process by selecting **Run console in FIPS mode** and clicking **Next**.

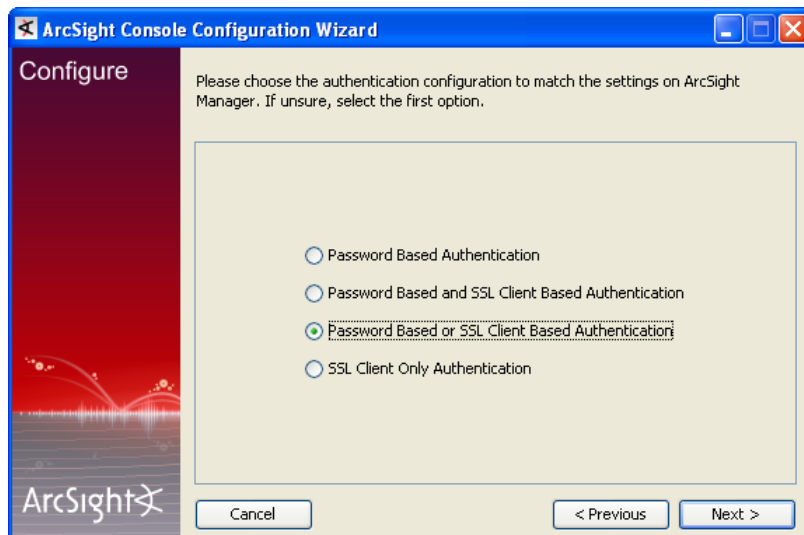
- 5 You will be reminded that once you select the FIPS mode, you will not be able to revert to the default mode. Click **Yes**.



- 6 You will be prompted to select a cipher suite. Select the type of FIPS the Manager uses and click **Next**.



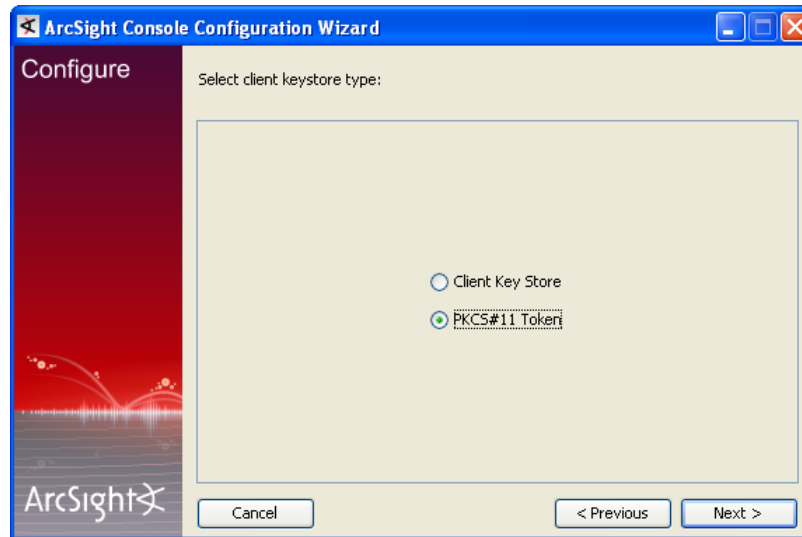
- 7 Next you will be prompted for the Manager's hostname and port. The Manager hostname must be the same (short name, fully qualified domain name, or IP address) as the Common Name (CN) you used when you created the Manager key pair.
- 8 Follow the prompts in the next few wizard screens (Refer to the "Installing ArcSight Console" chapter, earlier in this guide, for details on any screen) until you get to the screen where you have to select the authentication option.



Select the option that you had set on the Manager when installing it.



- 9 If you are using SSL client-based authentication and if you plan to use a PKCS #11 token with the Console, select **PKCS #11 Token** option in the following screen. Otherwise skip this step.



Enter the path or browse to the PKCS #11 library.

By default, the PKCS #11 library is located in the following directory:

On 32-bit Windows:

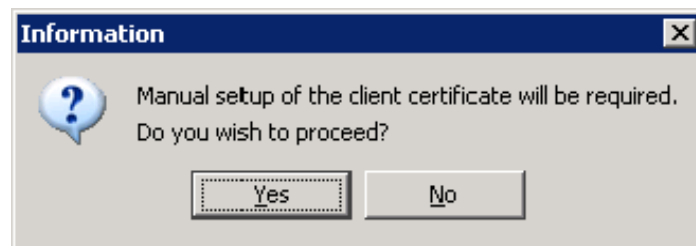
`C:\Program Files\ActivIdentity\ActivClient\acpkcs211.dll`

On 64-bit Windows:

`C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`

(this is the 32-bit version of the ActivClient library)

If you do not plan to use a PKCS #11 token with the Console, select **Client Key Store**, you will see a message reminding you to set up the client certificate after the installation completes.



After completing the Configuration Wizard, follow the procedure, [Setting up Client-Side Authentication](#) described in [Appendix E, Configuration Changes Related to FIPS](#), on [page 163](#), in the *Administrator's Guide* to set up the client certificate.

- 10 Follow the prompts in the next few wizard screens to complete the Console installation. Refer to the "Installing ArcSight Console" chapter, earlier in this guide, for details on any screen.



Note

If you have installed the product in FIPS with Suite B mode, select Firefox as your default browser when installing the Console on Windows. You cannot use the Internet Explorer browser because it does not support FIPS with Suite B.

When you start the Console, you should see a message saying that the Console is being started in FIPS mode.

## Connecting a Default Mode Console to a FIPS 140-2 Manager

To have an ArcSight Console installed in the default mode to connect to a Manager running in the FIPS 140-2 mode:

- Either add `server.fips.enabled=true` in your `console.properties` file located in the Console's `<ARCSIGHT_HOME>/current/config` directory...  
Or add `-Dhttps.protocols=TLSv1` to the `ARCSIGHT_JVM_OPTIONS` variable in the Console's `<ARCSIGHT_HOME>/current/bin/scripts/console.sh` file.
- import the Manager's certificate into `\current\jre\lib\security\cacerts` on the Console using the `keytoolgui` tool. See section, "Using Keytoolgui to Import a Certificate" in the *Administrator's Guide* for details on how to do this.



Caution

Once you configure your Console running in Default mode to connect to a FIPS enabled Manager by following the steps above, you will not be able to connect this Console to a Manager running in Default mode without reversing the changes you made to the files.



Note

You cannot connect a default mode ArcSight Console to a Manager using FIPS Suite B.

---

## Connecting a FIPS Console to FIPS Enabled Managers

This procedure should be automatic for multiple managers. Just make sure that each Manager certificate has a unique Common Name (CN) so that it's CN does not conflict with the CN of any existing certificate in the Console's `nssdb.client`.

If you need to import a Manager's certificate into the Console's `nssdb.client` manually, refer to the *Administrator's Guide* for details on the procedure.

## Configure Your Browser for FIPS

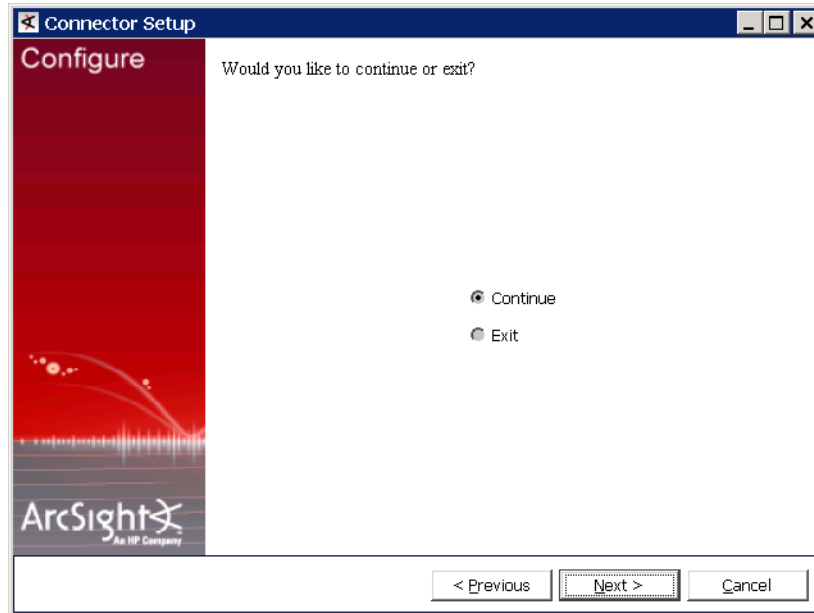
To connect a browser to a FIPS web server, the browser must be configured to support FIPS. Review the documentation for your browser and follow the instructions to make it FIPS compliant before using it for ArcSight Console online help or to connect to ArcSight Web or the Management Console.

If you are using Firefox 13.x or later, you must change two preferences `network.http.spdy.enabled` to `false`.

- 1 In the URL address window type `about:config`.
- 2 Find the preference "network.http.spdy.enabled."
- 3 If the value is `true`, double click the entry to change it to `false`.
- 4 In all versions of Firefox, find the preference "security.enable\_tls\_session\_tickets."
- 5 If the value is `true`, double click the entry to change it to `false`.

## Installing SmartConnectors in FIPS mode

When the Manager is installed in FIPS mode, the SmartConnectors must also be installed in FIPS mode. When you run the SmartConnector installation, continue until you see the screen below. Select the "Exit" and click **Next** to quit the installation. You have to import the Manager's certificate to allow the connector to trust the Manager before adding a new connector.



To import the Manager's certificate, run the following command from the connector's `<ARCSIGHT_HOME>/current/bin` directory:

```
./arcsight runcertutil -A -d
<ARCSIGHT_HOME>/current/user/agent/nssdb.client -n mykey -t
"CT,C,C" -i <absolute_path_to_managercertificatename.cert>
```

Enter "changeit" (without quotes) for password when prompted.

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

```
./arcsight runcertutil -A -d
<ARCSIGHT_HOME>/current/user/agent/nssdb.client -n mykey -t
"CT,C,C" -i /opt/arcsight/smartconnector/ManagerCert.cer
```

Run `runagentsetup` to resume your connector setup.

For more information on installing SmartConnectors in FIPS mode see *Installing FIPS-Compliant SmartConnectors*. It is used in conjunction with the individual device SmartConnector configuration guides for your device.

## How do I Know If My Installation is FIPS Enabled?

To figure out whether your existing installation has been installed in FIPS mode or default mode, check the `fips.enabled` property in the component's property file located as follows:

- `/opt/arcsight/manager/config/server.properties` for the Manager
- `<ARCSIGHT_HOME>/current/config/console.properties` for the ArcSight Console
- `/opt/arcsight/web/config/webserver.properties` for the ArcSight Web console

If FIPS mode is enabled, the property should be set to `fips.enabled=true`. If the component is running in default mode, the property will be set to `false`.

# Index

---

## A

- appendix
  - example of 69, 81
- ArcSight
  - Manager 7
- ArcSight Console
  - client authentication 40
  - connecting to the Manager 38
  - installing 33, 34
  - reconfiguring 47
  - reconnecting to Manager 46
  - starting 44
  - uninstalling 47
  - user logs and preferences 42
  - web browser configuration 41
- ArcSight Manager
  - default settings 66
  - setup 59

## C

- changing
  - host name 62
  - IP address 61
- character set 36
- client authentication
  - ArcSight Console 40
- configuration
  - web browser in Console 41
- connecting
  - ArcSight Console to Manager 38
- Console
  - installing 34
  - supported platforms 33
- customizing
  - components 59

## D

- default settings
  - ArcSight Manager 66
- Deployment Overview 8

## E

- ESM 7
  - components 7
  - effects of communication when components fail 9
  - overview 7

## F

- First Boot Wizard
  - fatal error 60

## H

- host name, changing 62
- hot key issue 36

## I

- installing
  - ArcSight Console 34
- IP address, changing 61

## M

- Manager 7
  - transferring configuration 36

## P

- passwords
  - character set 36
- preferences
  - ArcSight Console 42

## R

- reconfiguring
  - ArcSight Console 47
- reconnecting
  - Console to Manager 46
- restarting
  - First boot wizard 28

## S

- setup
  - ArcSight Manager 59
- shortcut key issue 36
- SmartConnectors 49
- starting
  - ArcSight Console 44
- supported platforms
  - Console 33

## T

- Troubleshooting 57
  - fatal error 60

## U

- uninstalling
  - ArcSight Console 47
- user logs
  - ArcSight Console 42

## W

- Web browser
  - configuring in Console 41
- wizard
  - restarting 28