

# **Installation and Configuration Guide**

---

Command Center

ArcSight ESM 6.5c

October 15, 2013



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

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

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

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

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

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

This document is confidential.

## Contact Information

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

## Revision History

Date	Product Version	Description
10/15/2013	ESM with CORR-Engine 6.5c	Updated the book to reflect the changes for ESM 6.5c

# Contents

---

<b>Chapter 1: What is ESM with CORR-Engine Storage?</b>	<b>7</b>
ESM Components	7
Manager	7
CORR-Engine	8
ArcSight Command Center	8
ArcSight Console	8
SmartConnectors	8
ArcSight Web	8
Deployment Overview	9
ESM Communication Overview	9
Effect on Communication when Components Fail	9
Choosing between FIPS Mode or Default Mode	10
Mode Comparison	10
Using PKCS#11	11
Import Control Issues	11
Directory Structure for ESM Installation	11
Securing Your ESM System	12
Protecting ArcSight Manager	12
ArcSight Built-In Security	13
Physical Security for the Hardware	13
Operating System Security	14
General Guidelines and Policies about Security	14
<b>Chapter 2: Installing ESM</b>	<b>17</b>
System Requirements	17
Supported Platforms	18
Before you Install ESM	18
Keep these TCP ports Open	18
Preparing to Install	18
The /tmp Directory Size	19
Sizing Guidelines for CORR-Engine	19
Create "arcsight" User	19
/opt/arcsight Directory	20
Write and Execute Permission for /opt/arcsight/	20

Execute Permission to /sbin for user 'arcsight'	20
Increase User Process Limit	20
Installing ESM	21
Running the Installation File	21
Rerunning the Suite Installer	25
Running the First Boot Wizard in Console Mode	25
Configuration	25
Changing the Manager Heap Size	34
Rerunning the Wizard	34
Uninstalling ESM	34
To Set Up ESM Reports to Display in a Non-English Environment	35
On the Manager	35
On the Console	35
Improving the Performance of Your Server	36
The Next Steps	36
<b>Chapter 3: Installing ArcSight Console</b>	<b>37</b>
Console Supported Platforms	37
Required Libraries on the RHEL 6.4 64 Bit Workstation	37
Using a PKCS#11 Token	38
Installing the Console	38
Configuration Settings	40
Selecting the Mode in which to Configure ArcSight Console	40
Manager Connection	41
Authentication	44
Web Browser	45
Importing the Console's Certificate into the Browser	48
Character Set Encoding	48
To Set Up ESM Reports to Display in a Non-English Environment	49
Starting the ArcSight Console	49
Logging into the Console	51
Reconnecting to the ArcSight Manager	51
Reconfiguring the ArcSight Console	52
Uninstalling the ArcSight Console	52
<b>Appendix A: Troubleshooting</b>	<b>53</b>
Location of Log files for Components	53
If you Encounter an Unsuccessful Installation	55
Customizing ESM Components Further	55
Fatal Error when Running the First Boot Wizard	56
Changing the IP Address of Your Machine	56
Changing the Host Name of the Machine	
After Running the First Boot Wizard	58

<b>Appendix B: Default Settings for Components .....</b>	<b>61</b>
General .....	61
CORR-Engine .....	61
Manager .....	62
ArcSight Web .....	63
<b>Appendix C: Using the PKCS#11 Token .....</b>	<b>65</b>
What is PKCS? .....	65
PKCS#11 .....	65
PKCS#12 .....	65
PKCS#11 Token Support in ESM .....	66
References to <ARCSIGHT_HOME> .....	66
Setting Up to Use a CAC Card .....	66
Install the CAC Provider's Software .....	66
Map a User's External ID to the CAC's Subject CN .....	67
Obtain the CAC's Issuers' Certificate .....	69
Extract the Root CA Certificate From the CAC Certificate .....	70
Import the CAC Root CA Certificate into the ArcSight Manager .....	71
FIPS Mode - Import into the ArcSight Manager's nssdb .....	72
Default Mode - Import into the ArcSight Manager's Truststore .....	72
Select Authentication Option in ArcSight Console Setup .....	73
Logging in to the ArcSight Console Using CAC .....	74
Logging in to the ArcSight Command Center Using CAC .....	74
Using CAC with ArcSight Web .....	75
<b>Appendix D: ESM in FIPS Mode .....</b>	<b>77</b>
What is FIPS? .....	77
Network Security Services Database (NSS DB) .....	78
What is Suite B? .....	78
NSS Tools Used to Configure Components in FIPS Mode .....	79
TLS Configuration in a Nutshell .....	79
Understanding Server Side Authentication .....	80
Understanding Client Side Authentication .....	80
Setting up Authentication on ArcSight Web - A Special Case .....	80
Exporting the ArcSight Manager's certificate for Other Clients .....	80
References to ARCSIGHT_HOME .....	81
Using PKCS #11 Token With a FIPS Mode Setup .....	81
Installing ArcSight Console in FIPS Mode .....	82
Connecting a Default Mode ArcSight Console to a FIPS 140-2 ArcSight Manager .....	85
Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers .....	86
Configure Your Browser for FIPS .....	86
FIPS with Firefox .....	86
Installing SmartConnectors in FIPS mode .....	88

How do I Know If My Installation is FIPS Enabled? ..... 89

**Index ..... 91**

# 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 9](#)

["ESM Communication Overview" on page 9](#)

## ESM Components

The ESM system comprises of the following components:

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

### Manager

The 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.

## CORR-Engine

The 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 Command Center

The ArcSight Command Center is a web-based user interface for ESM. This user interface has the following characteristics:

- ArcSight Command Center enables you to perform many of the functions found in the ArcSight Console and ArcSight Web, which are still provided with ESM.
- It provides dashboards, several kinds of searches, reports, case management, notifications, and administrative functions for managing content, users, connectors, storage, archives, search filters, saved searches, and peer configuration.
- It has taken over functions from the Management Console. If you used that console with a previous ESM release, switch to the ArcSight Command Center.

## 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.

## SmartConnectors

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

## ArcSight Web

ArcSight Web is a web server that enables you to access the Manager securely using a browser.

ArcSight Web is intended for users who need to view information on the Manager, but not author or administer it; for example, operators in a Security Operations Center (SOC) and customers of a Managed Security Service Provider (MSSP).

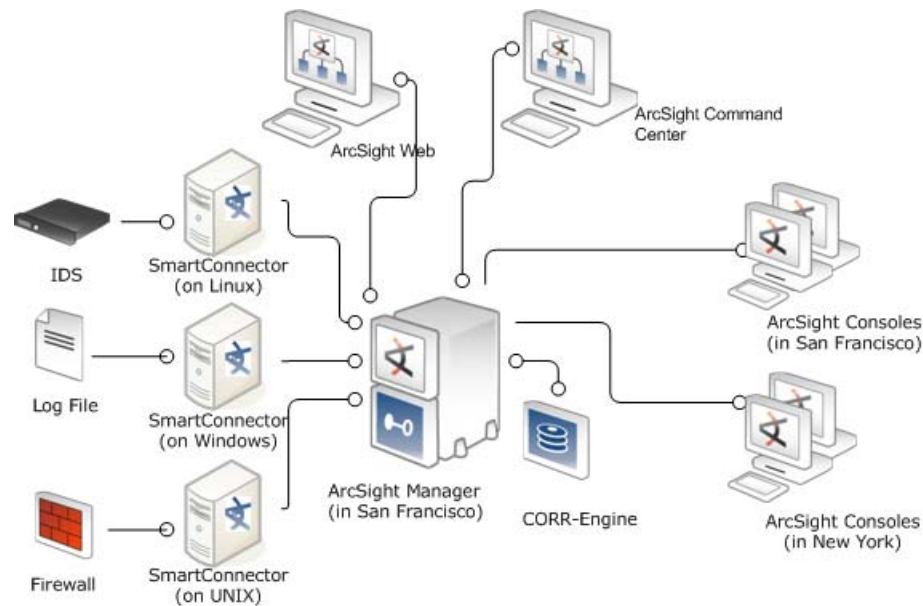
ArcSight Web can be installed on the same server as the Manager or on a separate server that has network access to the Manager. If ArcSight Web is installed on a separate server, that server makes secure connections to the Manager on behalf of the browsers requesting data from the Manager.

If the separately installed server is accessible from outside of a protected network, users from outside of that network can use ArcSight Web to access information on the Manager.



## Deployment Overview

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



**Figure 1-1** ESM Deployment

## ESM Communication Overview

The ArcSight Console, Manager, and SmartConnectors 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 the 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"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> <li>• More...</li> </ul>	Keypair and Certificates stored in Keystore and cacerts, and Truststore in JKS format
FIPS 140-2 Mode	TLS	<ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul>	Keypair and Certificates stored in NSSDB
FIPS with Suite B Mode	TLS	<ul style="list-style-type: none"> <li>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA Suite B 128 bits security level, providing protection from classified up to secret information</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA Suite B 192 bits security level, providing protection from classified up to top secret information</li> </ul>	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 ESM 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 ESM'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.

## Directory Structure for ESM Installation

By default, the ESM software gets installed in a directory tree under a single root directory. Other third-party software is not necessarily installed under this directory, however. The path to this root directory is called `/opt/arcsight`.

The directory structure below `/opt/arcsight` is also standardized across components and platforms. The following table lists a few of the commonly used directories across the components.

Port	Directory
ESM Software	<code>/opt/arcsight/&lt;component&gt;/bin</code>
Properties files	<code>/opt/arcsight/&lt;component&gt;/config</code>
Log files	<code>/opt/arcsight/&lt;component&gt;/logs</code>

## Securing Your ESM System

Follow the information in the following sections to protect your ArcSight components.



Note

By default, the minimum length for passwords is six characters and the maximum length is 20 characters. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration," "password Character Sets."

### Protecting ArcSight Manager

Don't use demo SSL certificates in production. Make sure when switching that you remove the demo CA from cacerts on all SmartConnectors and ArcSight Consoles.

Closely control access to files, using the principle of least privilege, which states that a user should be given only those privileges that the user needs to complete his or her tasks. The following files are particularly sensitive:



Note

<ARCSIGHT\_HOME> is the root directory for the Manager component:  
/opt/arcsight/manager

- <ARCSIGHT\_HOME>\config\jetty\keystore (to prevent the ArcSight Manager private key from being stolen)
- <ARCSIGHT\_HOME>\config\jetty\truststore (w/ SSL Client authentication only, to prevent injection of new trusted CAs)
- <ARCSIGHT\_HOME>\config\server.properties (has keystore and database passwords)
- <ARCSIGHT\_HOME>\config\jaas.config (w/ RADIUS or SecurID enabled only, has shared node secret)
- <ARCSIGHT\_HOME>\config\client.properties (w/ SSL Client authentication only, has keystore passwords)
- <ARCSIGHT\_HOME>\reports\sree.properties (to protect the report license)
- <ARCSIGHT\_HOME>\reports\archive\\* (to prevent archived reports from being stolen)
- <ARCSIGHT\_HOME>\jre\lib\security\cacerts (to prevent injection of new trusted CAs)
- <ARCSIGHT\_HOME>\lib\\* (to prevent injection of malicious code)
- <ARCSIGHT\_HOME>\rules\classes\\* (to prevent code injection)

Use a host-based firewall. On the ArcSight Manager, block everything except for the following ports. Make sure you restrict the remote IP addresses that may connect to those that actually need to talk.

Port	Flow	Description
22/TCP	Inbound	SSH log in (Unix only)
53/UDP	Inbound/Outbound	DNS requests and responses
8443/TCP	Inbound	SmartConnectors and Consoles

Port	Flow	Description
25/TCP	Outbound	SMTP to mail server
110/TCP	Outbound	POP3 to mail server, if applicable
143/TCP	Outbound	IMAP to mail server, if applicable
1645/UDP	Inbound/Outbound	RADIUS, if applicable
1812/UDP	Inbound/Outbound	RADIUS, if applicable
389/TCP	Outbound	LDAP to LDAP server, if applicable
636/TCP	Outbound	LDAP over SSL to LDAP server, if applicable

As another layer of defense (or if no host-based firewall is available), you can also restrict which connections are accepted by the ArcSight Manager using the following properties in the `server.properties` file:

```
web.accept.ips=
xmlrpc.accept.ips=
agents.accept.ips=
```

Each of these properties takes a list of IP addresses or subnet specifications, separated by commas or spaces. Once specified, only connections originating from those addresses are accepted. The `xmlrpc.accept.ips` property restricts access for ArcSight Consoles and the ArcSight Web server. The `agents.accept.ips` property restricts access for SmartConnectors. For registration, the SmartConnectors need to be in `xmlrpc.accept.ips` as well, so that they can be registered. The format for specifying subnets is quite flexible, as shown in the following example:

```
web.accept.ips=192.168.10.0/24 192.168.30.171
xmlrpc.accept.ips=192.168.10.120 192.168.10.132
agents.accept.ips=10.*.*.*,192.168.0.0/255.255.0.0
```

## ArcSight Built-In Security

HP ArcSight user accounts have user types that control the functions which users can access in the ArcSight Manager. The "Normal User" type has the most privileges. Where possible, use more restrictive types, such as "Manager SmartConnector," "Management Tool," or "Archive Utility" for non-human user accounts. This is particularly important when user passwords must be stored in scripts for unattended execution.

Apply the principle of least privilege when creating user accounts in ESM and when granting access to resources or events. Users should not have more privileges than their tasks require.

## Physical Security for the Hardware

In addition to establishing security policies for passwords, keystores, and other software facilities, it is important to provide physical security for the hardware used by the ESM system. Physical hardware includes computers running ArcSight Console, and SmartConnector software, as well as the network which connects them.

Physical access to computers running ArcSight software must be restricted.

- Use the locking mechanisms provided by most rackmount cases to prevent malicious/accidental tampering with the machine.
- Use locks on disk drive enclosures.
- Use redundant power and uninterruptible power supplies (UPS).
- Protect the BIOS (x86 systems only) or firmware:
  - ◆ Disable all CD-ROM drives for booting so that the system can only be booted from the hard disk.
  - ◆ Disable COM, parallel, and USB ports so that they can't be used to extract data.
  - ◆ Disable power management.

## Operating System Security

- On Linux, set up a boot loader password to prevent unauthorized people from booting into single user mode (see the LILO or GRUB documentation for details).
- On Linux, disable reboot by Ctrl-Alt-Del in `/etc/inittab`. Comment out the line that refers to "ctrlaltdel."
- Set up a screen saver that prompts for a password with a moderately short delay (such as five minutes).
- Disable power management in the OS.
- When installing the OS, select packages individually. Only install what you know will be needed. You can always install missing packages as you encounter them.
- Run automated update tools to obtain all security fixes. Use `up2date` on Red Hat Linux (may require Red Hat Network subscription).
- Uninstall (or at least turn off) all services that you don't need. In particular: finger, r-services, telnet, ftp, httpd, linuxconf (on Linux), Remote Administration Services and IIS Services on Windows.
- On Unix machines, disallow remote root logins (for OpenSSH, this can be done using the `PermitRootLogin no` directive in `/etc/ssh/sshd_config`). This will force remote users to log in as a non-root user and `su` to root, thus requiring knowledge of two passwords to gain root access to the system. Restrict access to `su`, using a "wheel group" pluggable authentication module (PAM) so that only one non-root user on the machine can `su` to root. Make that user different from the "arcsight" user. That way, even if the root password is known and an attacker gains access through ESM in some way, they won't be able to log in as root.
- Rename the Administrator/root account to make brute force attacks harder.

## General Guidelines and Policies about Security

Educate system users about "social engineering" tricks used to discover user account information. No employee of HP will ever request a user's password. When HP representatives are on site, the administrator of the system will be asked to enter the password and, if needed, to temporarily change the password for the HP team to work effectively.

Educate users to use secure means of communication—such as SSL to upload to `software.arcsight.com` or PGP for e-mail—when transferring configuration information or log files to HP.

Set up a login banner stating the legal policies for use of the system and the consequences of misuse. (Instructions for creating a login banner vary by platform.) ArcSight Consoles

can also display a custom login banner. Contact the Customer Support using the HP SSO site for more information.

Choose secure passwords. (No password used in two places, seemingly random character sequences, eight characters or longer, containing numbers and special (non-letter) characters). For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration."

Passwords are used in the following places—if any one is breached, the system is compromised:

- All database accounts (arcsight)
- The "arcsight" user and root user on the system that runs the ArcSight Manager
- All users created in ESM
- The SSL keystores
- The boot loader (Linux)
- The BIOS (x86 systems only)
- The RADIUS node secret
- The LDAP password for ArcSight Manager (w/ basic authentication only), where applicable
- The Active Directory domain user password for ArcSight Manager where applicable

Consider purchasing and using a PKI solution to enable SSL client authentication on Consoles and SmartConnectors.

Consider purchasing and using a two-factor authentication solution such as RSA SecurID.

Make sure that all the servers with which ESM interacts (DNS, Mail, RADIUS, etc.) are hardened equivalently.

Use a firewall and intrusion detection systems to secure the network that runs the ArcSight Manager and ArcSight Database.





## Chapter 2

# Installing ESM

This chapter covers the following topics:

- [“System Requirements” on page 17](#)
- [“Before you Install ESM” on page 18](#)
- [“Preparing to Install” on page 18](#)
- [“Installing ESM” on page 21](#)
- [“Uninstalling ESM” on page 34](#)
- [“To Set Up ESM Reports to Display in a Non-English Environment” on page 35](#)
- [“The Next Steps” on page 36](#)

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

## System Requirements

The hardware requirements for ESM 6.5c 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)	1.5 TB disk space (RAID 10)	<= 8 TB (RAID 10)
	15,000 RPM	15,000 RPM	15,000 RPM



### Caution

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 Sales or Field Representative.

If you anticipate that you will have large lists (a list with roughly 5 million entries) or 500,000 Actors, ensure that your system meets the High Performance requirements above.

## Supported Platforms

ESM 6.5c is supported on Red Hat Enterprise Linux 6.4 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.



Note

- If you would like to install the product in GUI mode, you will also need to install X Window system package (`xorg-x11-server-utils-7.5-13.el6.x86_64`) on your machine if it does not already exist.
- RHEL 6.4 comes with the 2012j tzdata package by default, but you can update this RPM to 2013c if your timezone related changes are present in the 2013c package.

## Before you Install ESM

Before you begin to install ESM, do the following:

- The ESM 6.5c 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.



Note

You do not need to unzip the license zip file. ESM recognizes the license file in the zipped state.

- Both XFS as well as EXT4 file system formats are supported in ESM 6.5c.

## 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

9000

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

1976, 28001, 2812, 3306, 5555, 6005, 6009, 6443, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8808, 8880, 8888, 8889, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9123, 9124, 9999, 45450, 9095, 9090, 8766

## Preparing to Install

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

## The /tmp Directory Size

Make sure that the partition in which your **/tmp** directory resides has at least 3 GB of space.

## Sizing Guidelines for CORR-Engine

When installing ESM 6.5c, 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

**Total Space** - the total size of the disk partition. Detected automatically

**Reserved Space** - used for system internal use. By default, this is 10% of Total Space

**Usable Space** -Total Space minus Reserved Space

	Recommended	Minimum	Maximum
<b>System Storage Size</b>	One-sixth of usable space	3 GB	500 GB
<b>Event Storage Size</b>	Four-sixths of usable space	10 GB	8 TB
<b>Online Event Archive Size</b>	Remaining space after the System and Event storage have been allocated	1 GB	No limit



**Note**

### 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.

## /opt/arcsight Directory

ESM 6.5c gets installed in `/opt/arcsight/`. If the `/opt/arcsight/` directory does not exist, create it while logged in as a 'root' user.

## 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 while logged in as 'root':

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

## Execute Permission to /sbin for user 'arcsight'

Make sure to grant execute permission for the 'arcsight' user on the following directories by running the following while logged in as 'root':

```
chmod +x /sbin
chmod +x /sbin/ifconfig
chmod +x /sbin/lspci
chmod +x /usr/sbin
```

The permissions after running the above commands should look like `rxwxr-xr-x` for the above directories.

## Increase User Process Limit

On the Red Hat 6.4 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.
  - Delete the line `root nproc unlimited` that is present in the file by default
- 

```
* 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
```

## Installing ESM



Note

- Using an ssh -X session to run the ESM 6.5c 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 6.5c 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 since you will be installing ESM on it.

### Important!

The .tar file should be owned by the user "arcsight".

- c Change directory to the location where you downloaded the .tar file.
- d 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.



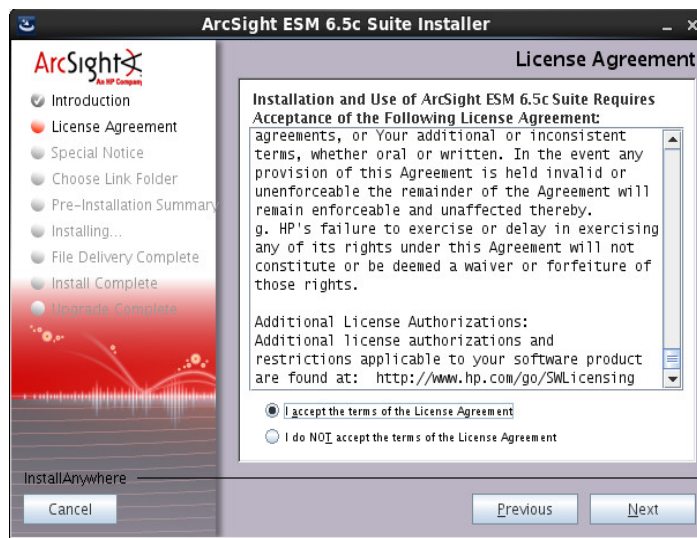
Note

- 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**.



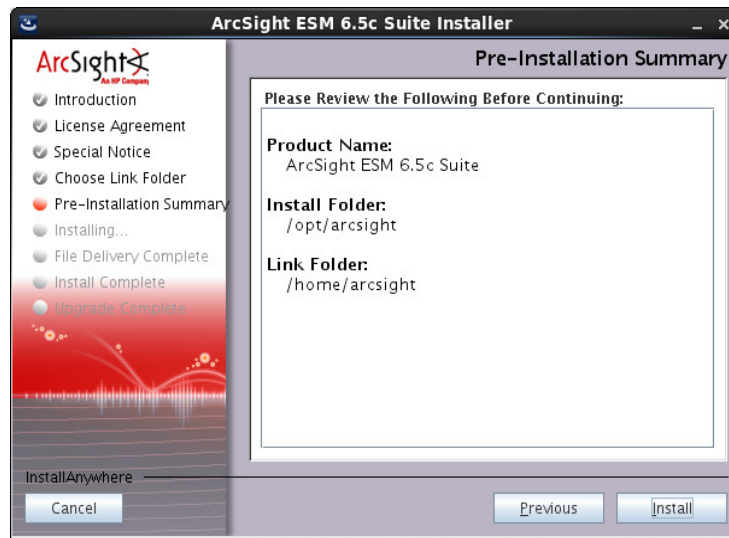
- 4 Read the special notice and click **Next**.



- 5 Select the location where you would like the installer to place the links for this 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**.

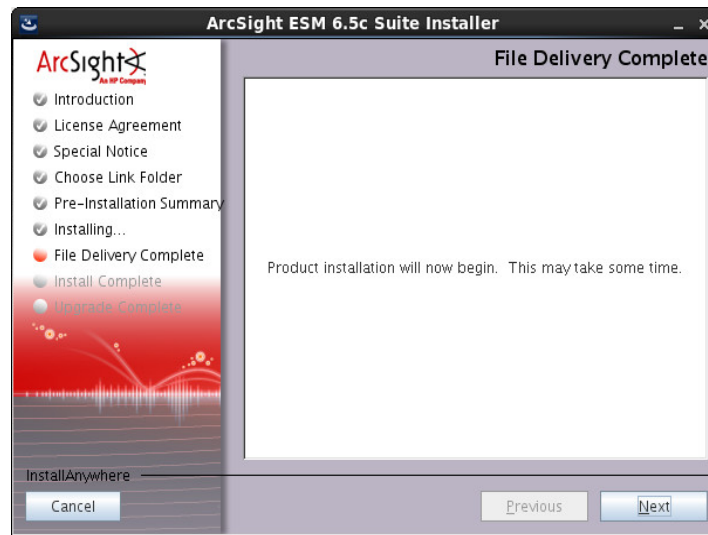


You will see the following progress bar.





- 7 The installer first places all the installation files in the appropriate folders. When it is done, a File Delivery Complete screen will open. 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.xxxx` 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
```



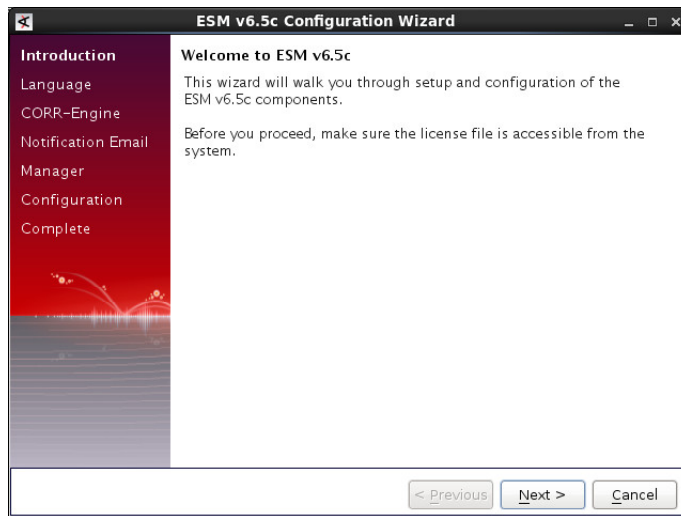
Make sure that X-Windows is not running when running the first boot wizard in console mode.

**Note**

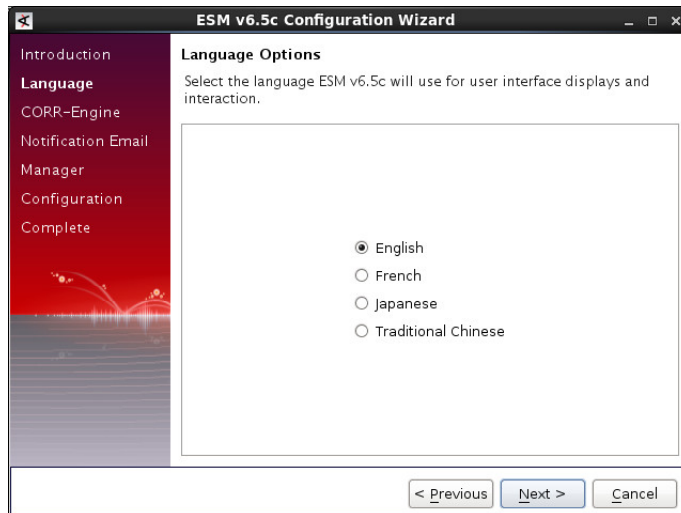
## Configuration

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**.



**Note**

- 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 ArcSight Command Center after you have installed ESM. Refer to the ArcSight Command Center User's Guide for information on how to do so.

**System Storage Size** - the size of the storage space that will be set aside to store resources

**Event Storage Size** - the size of the storage space that will be set aside to store events

**Online Event Archive Size** - the maximum number of gigabytes of disk space for the event archives. This only applies to default online event archive.

**Retention Period** - the amount of time that you want to retain the events before they are purged from the system

- 5 Configure the following e-mail addresses:

**Error Notification Recipients:** The email address of the person who should receive email notifications in the event that the Manager goes down or encounters some other problem.

**From email address:** The email address that will be used to represent the sender of the email notifications.

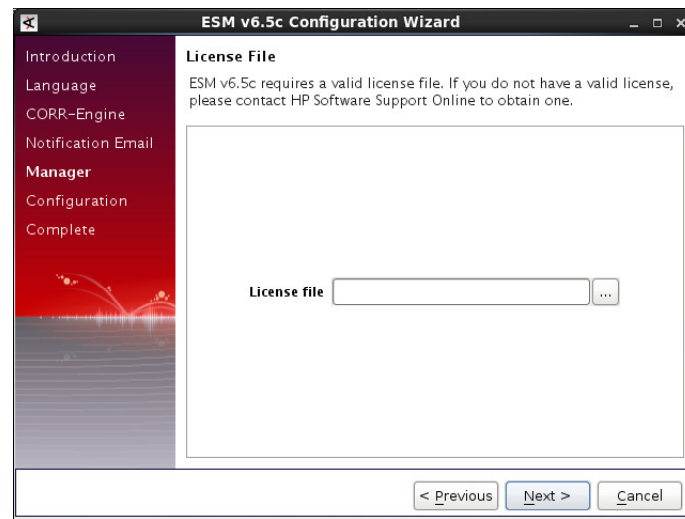
Click **Next**.

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

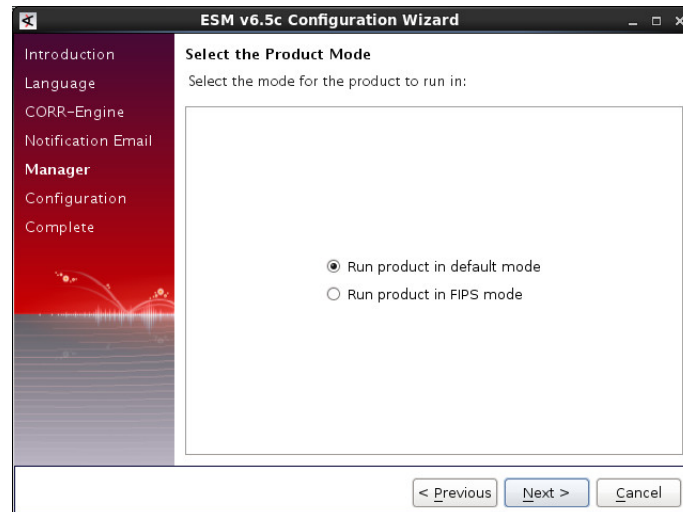


Note

If you have a valid existing ESM license, you can use it with ESM 6.5c.



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

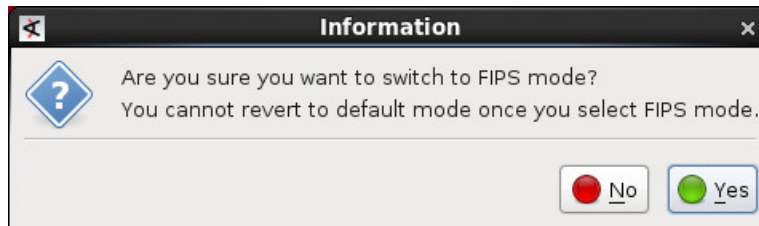


Click **Next**.

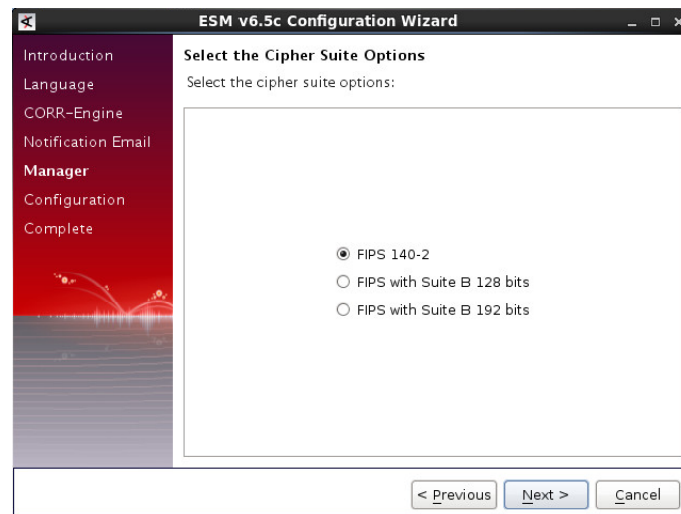


- If you choose to install the product in FIPS mode, be sure to install the Console in FIPS mode too. Refer to [“Installing ArcSight Console in FIPS Mode” on page 82](#) for instructions on installing the Console in FIPS mode.
- Once you have configured the software in FIPS-140 mode, you will not be 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 the following information asking you to confirm your selection.



- 9 **(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.

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

The screenshot shows the 'ESM v6.5c Configuration Wizard' window. On the left is a sidebar with a red background and white text listing the steps: Introduction, Language, CORR-Engine, Notification Email, **Manager**, Configuration, and Complete. The 'Manager' step is highlighted. 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.' Below this is a note: 'If you choose to provide a host name here, make sure it can be resolved through your Domain Name System (DNS) server.' There are four input fields: 'Manager host name (or IP)' (empty), 'Administrator user name' (containing 'admin'), 'Administrator password' (empty), and 'Password confirmation' (empty). At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.



**Caution**

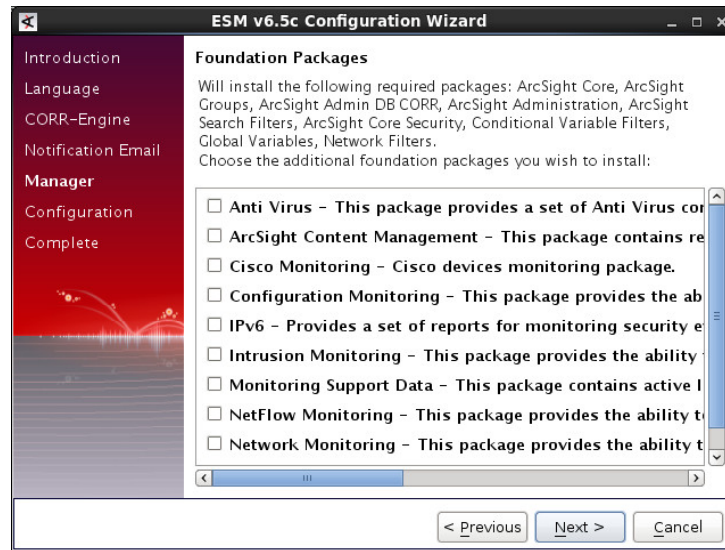
Manager host name is the local host name or IP address of the machine where the Manager gets installed. Note that this name is what all clients (for example, ArcSight Console) will need to specify to talk to the Manager. Using a host name instead of an IP address is recommended for flexibility.

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.

- 11** Select the system content packages that you would like to install. The System Content is now delivered in the form of packages. System content packages are automatically installed as a part of ESM to provide out-of-box resource suites that you can start using immediately to monitor and protect your network.

By default, the ArcSight Administration package that provides you information about your ESM installation is installed. You can select other packages to install from the list.

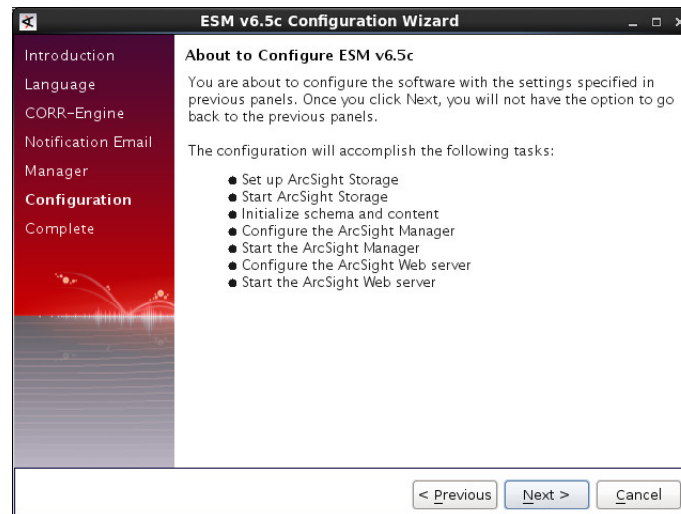


For more information about packages, see the ESM System Content Guide.

- 12** The next screen informs you of the ESM configuration steps that will be performed once you click Next in this screen. Read it and click **Next**.

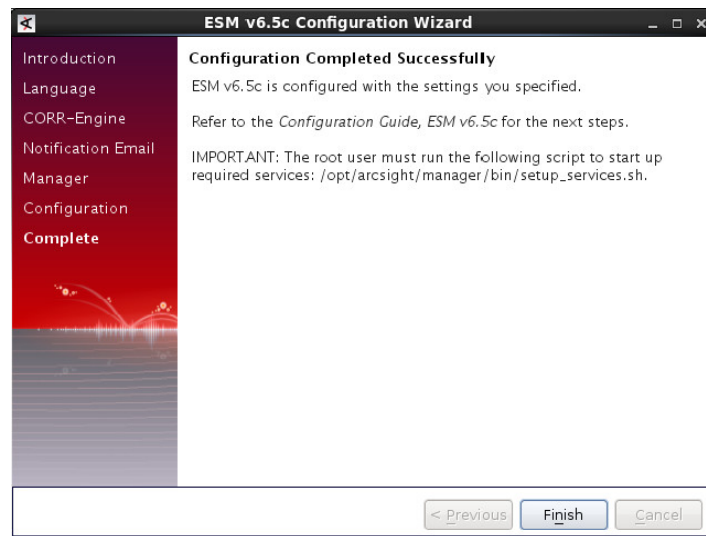


Review the selections you made in the previous screens of this wizard and make sure that they are to your satisfaction. Once you click Next, the product is installed as specified and cannot be changed.

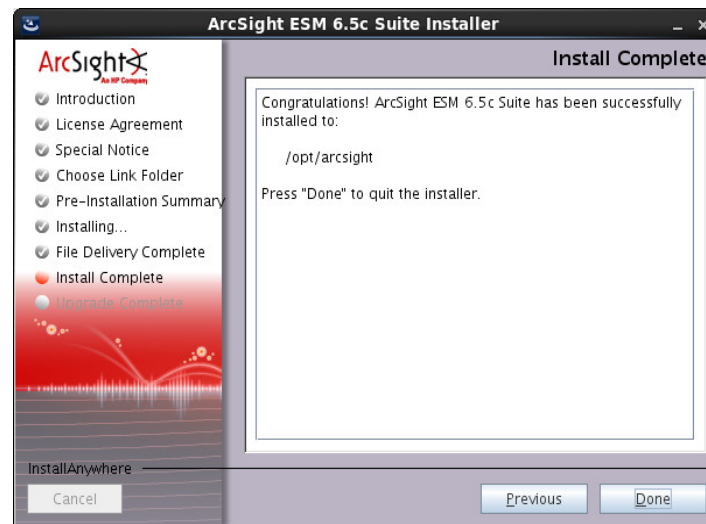




- 13** Upon successful configuration, you will see the Configuration Completed Successfully screen. Click **Finish**.



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



- 15 Important!** Log in as user “root” and run the following script to set up the required services:



This step is required in order to start the services.

**Caution**

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

After you have completed the installation, be sure to check the location and size of your storage volumes and make any necessary changes. You can do this in the ArcSight Command Center. Refer to the ArcSight Command Center User's Guide, the “Administration” chapter under “Storage and Archive” section for details regarding your storage volumes.

## 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 ArcSight Command Center. Refer to the ArcSight Command Center User's Guide for further details.

## 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 v6.5c" ([Step 12 on page 32](#)).

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_6.5
```

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

```
./Uninstall_ArcSight_ESM_Suite_6.5
```

- 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.

## 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
```

 Save the file.
- 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 machine.

- 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

## Improving the Performance of Your Server

For HP hardware, you can improve the server performance by tuning your BIOS as follows:

- **HyperThreading** - Disable this. This setting will exist on any Intel processor that supports HyperThreading. Most recent server class processors have this. AMD processors do not have an equivalent setting.
- **Intel VT-d** - Disable this. This setting is specific to Intel processors and will likely be present on most recent server class processors. AMD has an equivalent feature named AMD-Vi.
- **HP Power Regulator** - set to Static High Performance: This setting tells the CPU(s) to always run at high speed, rather than slowing down to save power when the system senses that load has decreased. Most modern CPUs have some equivalent setting.
- **Thermal Configuration** - set to Increased cooling: This setting increases fan speed in the server to help deal with the increased heat resulting from running the CPU(s) at high speed all the time.
- **Minimum Processor Idle Power Package State** - This setting tells the CPU not to use any of its C-states (various states of power saving in the CPU). All CPUs have C-states, so most servers will have a setting like this.
- **HP Power Profile** - set this to Maximum Performance. This is not likely to have an equivalent on non-HP servers, although some of the individual settings may exist.

This setting changes the following:

- ◆ QPI link power management (link between physical CPU sockets) gets disabled.
- ◆ PCIe support gets forced to Gen 2.
- ◆ C-states get disabled as part of this profile.
- ◆ This setting also disables the lower speed settings on the CPU(s) so they run at high speed all the time.

## 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 Manager from the ArcSight Command Center 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 ArcSight Command Center User's Guide for more information on using the ArcSight Command Center.

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 77](#). Section [“Mode Comparison” on page 10](#) lists the basic differences between the modes.

The following topics are covered in this chapter:

- [“Console Supported Platforms” on page 37](#)
- [“Using a PKCS#11 Token” on page 38](#)
- [“Installing the Console” on page 38](#)
- [“Starting the ArcSight Console” on page 49](#)
- [“Reconnecting to the ArcSight Manager” on page 51](#)
- [“Reconfiguring the ArcSight Console” on page 52](#)
- [“Uninstalling the ArcSight Console” on page 52](#)

Make sure the Manager 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 6.4 64 Bit Workstation

On the RHEL 6.4 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 65](#) for details on using a PKCS #11 token with the Console.

## Installing the Console



Caution

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.



Note

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 ESM 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	ArcSight-6.5.x.nnnnn.y-Console-Linux.bin
Windows	ArcSight-6.5.x.nnnnn.y-Console-Win.exe
Macintosh	ArcSight-6.5.x.nnnnn.y-Console-MacOSX.zip

- 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**

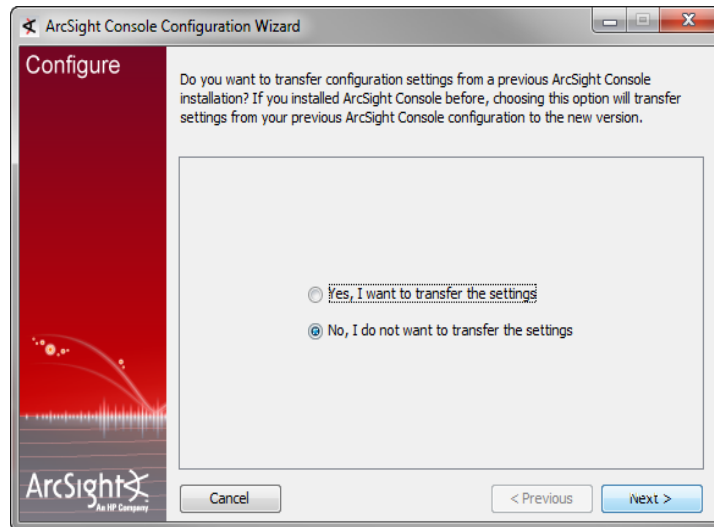
- On Linux and Macintosh systems, spaces are not supported in install paths for ESM 6.5c.
- **On Windows Vista (64-bit):** Make sure that you have administrative privileges to the C:\, C:\Program Files, and C:\Windows directories because these are protected folders and you will not be able to create 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.

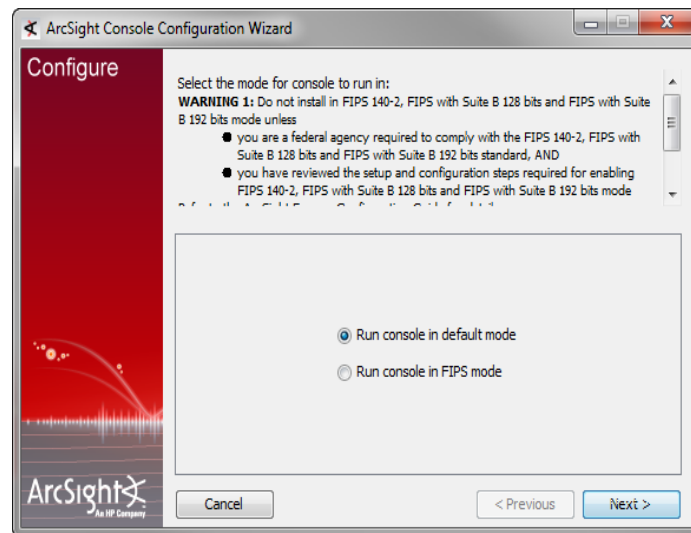
## Configuration Settings

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

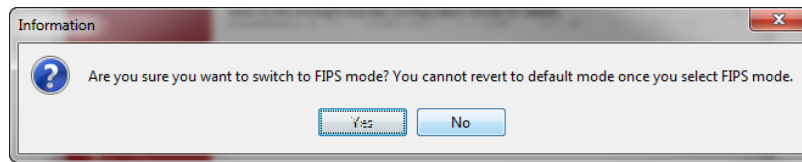
Next, you will see the following screen:



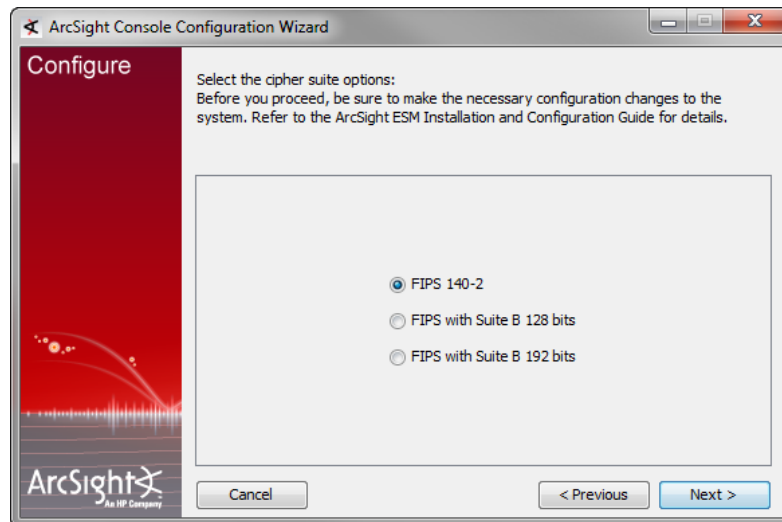
Select the mode in which to install the Console. This should be the same mode in which the Manager is installed.



**(FIPS mode only)** If you selected **Run console in FIPS mode**, you will get the following information pop-up.



**(FIPS mode only)** 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**.

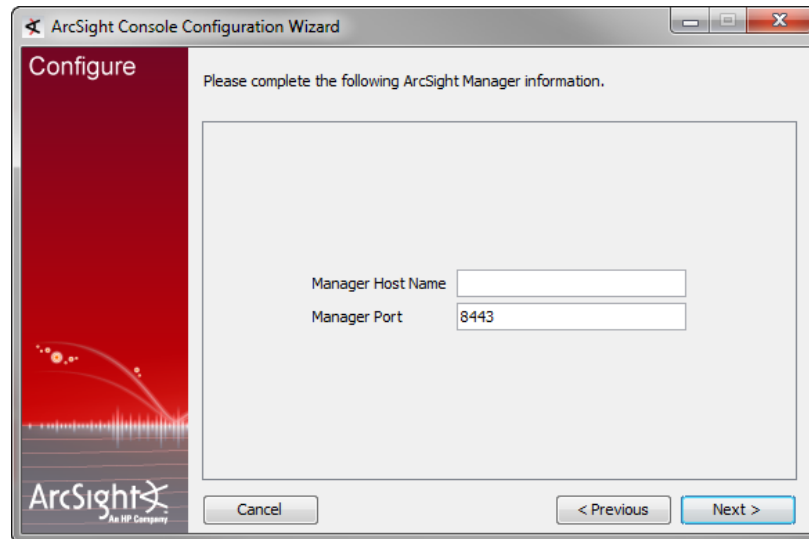
## Manager Connection

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.



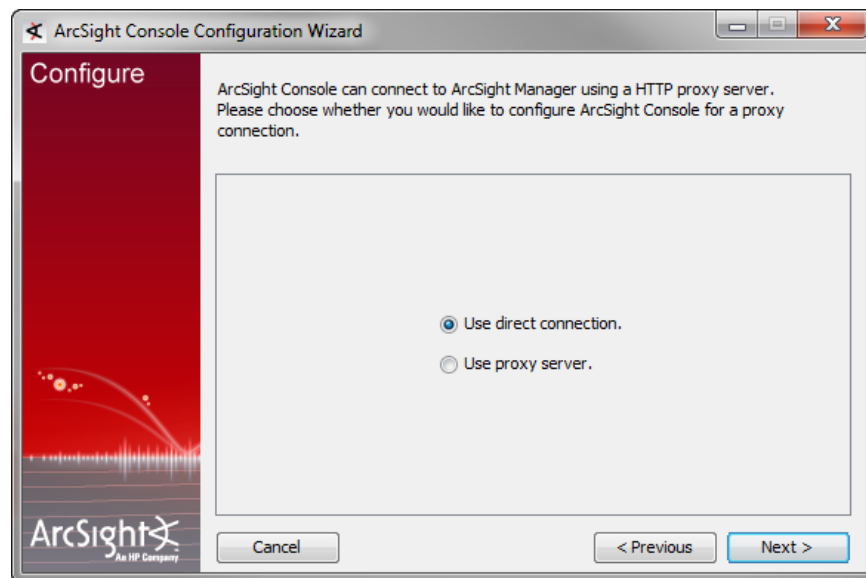
Do not change the Manager's port number.

Click **Next**.



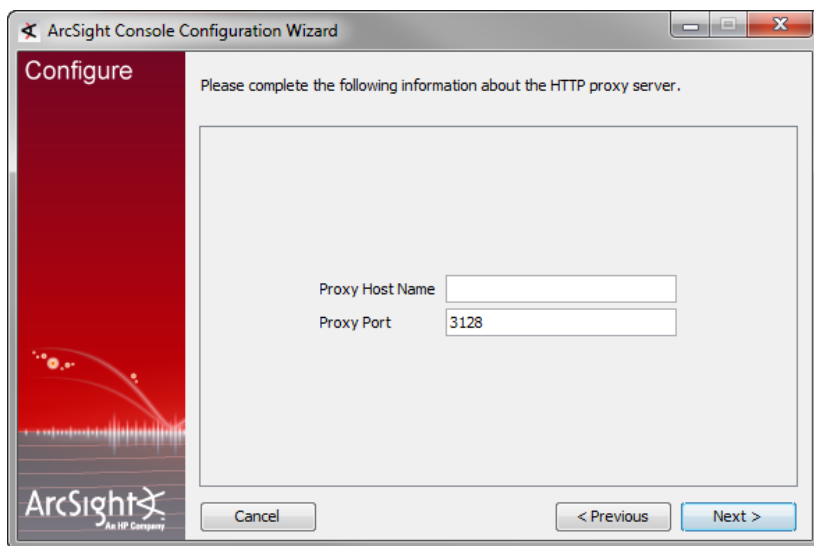
The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. On the left is a red sidebar with the ArcSight logo and 'An HP Company' text. The main area has a light gray background with the text 'Please complete the following ArcSight Manager information.' Below this is a form with two fields: 'Manager Host Name' and 'Manager Port'. The 'Manager Port' field contains the value '8443'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'. The 'Next >' button is highlighted in blue.

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.



The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard, specifically the connection options screen. The window title is 'ArcSight Console Configuration Wizard'. On the left is a red sidebar with the ArcSight logo and 'An HP Company' text. The main area has a light gray background with the text 'ArcSight Console can connect to ArcSight Manager using a HTTP proxy server. Please choose whether you would like to configure ArcSight Console for a proxy connection.' Below this is a form with two radio button options: 'Use direct connection.' (which is selected) and 'Use proxy server.' At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'. The 'Next >' button is highlighted in blue.

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 contains the text 'Please complete the following information about the HTTP proxy server.' Below this text 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 in blue.

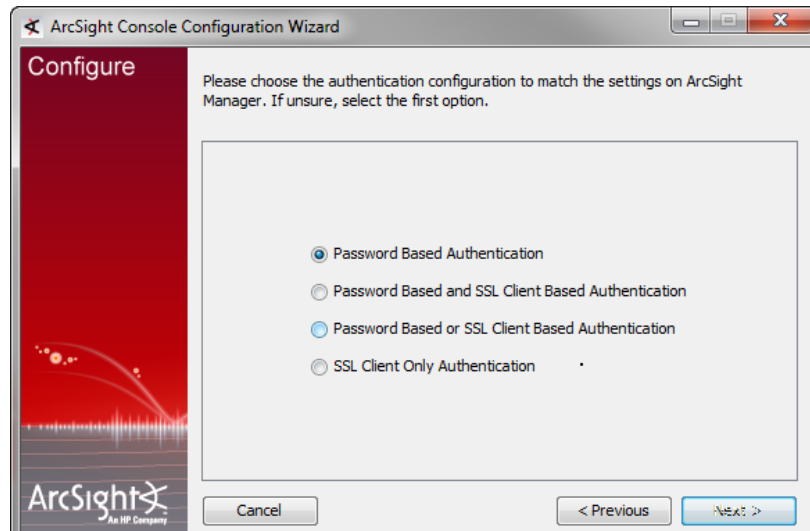
Enter the Proxy Host name and click **Next**.

## Authentication

**Caution**

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:

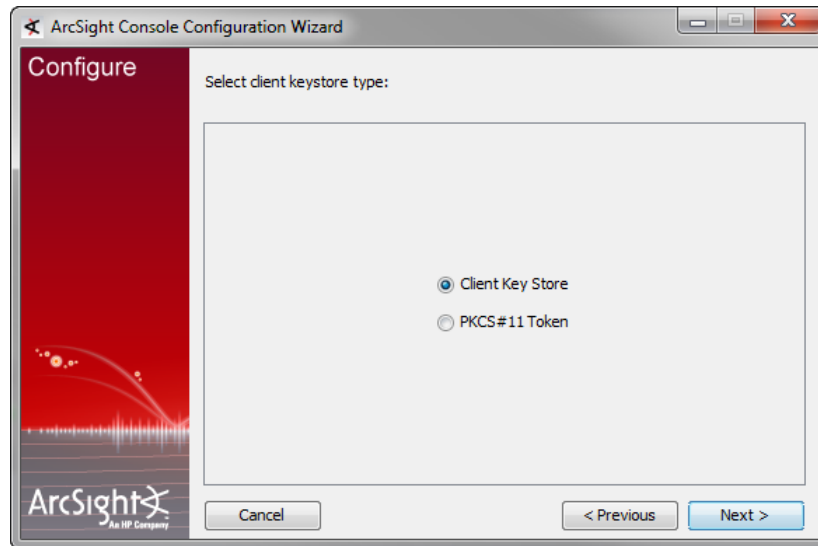
**Note**

**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.

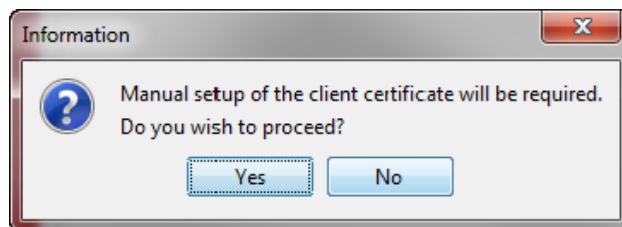
If you select **Password Based and SSL Client Based Authentication**, you will be required to enter both user name/password combination and you will be required to setup your client certificate manually. Follow the procedure described in ESM Administrator's Guide to set up the client certificate.

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 65](#) 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.

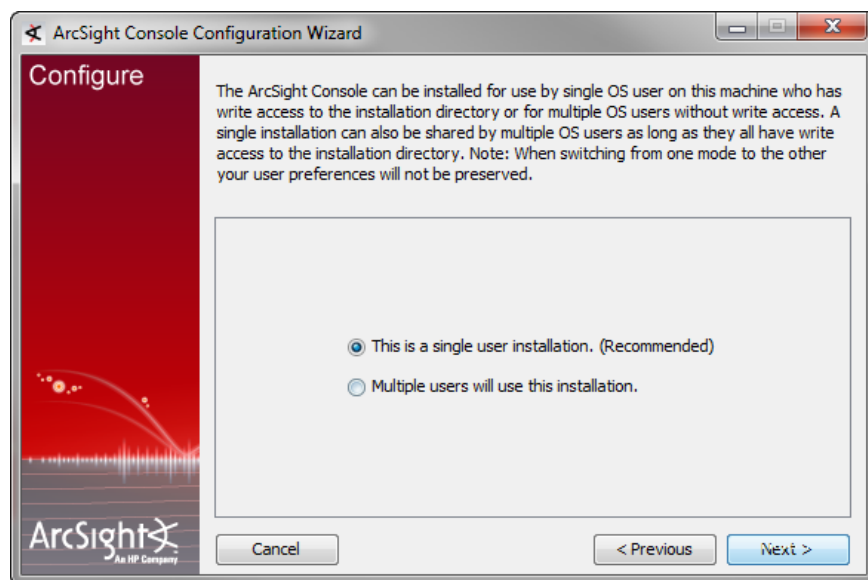
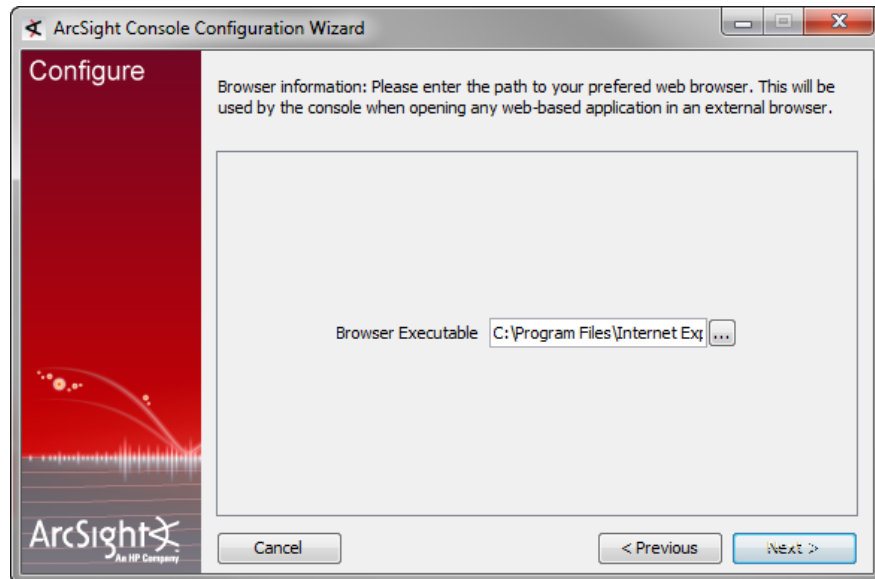


After completing the Configuration Wizard, follow the procedure described in ESM Administrator's Guide to set up the client certificate.

## 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:

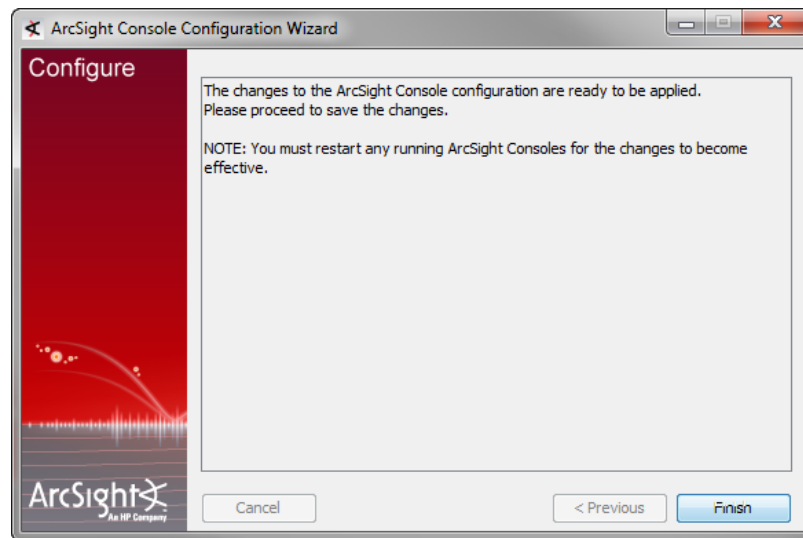
- ◆ `sendlogs`
- ◆ `console`
- ◆ `exceptions`
- ◆ `portinfo`
- ◆ `websearch`

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.

## 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.

## 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 ["On the Console" on page 35](#) will allow the international characters to be stored and recognized correctly by ESM.

## Starting the ArcSight Console



On the ArcSight Console machine, for any special IPV4/IPV6 configurations that do not match the DNS server entries, you can instruct the ArcSight Console how to connect to ESM by providing an additional option `java.net.preferIPv6Addresses`. Do that by setting the environment variable `ARCIGHT_JVM_NET_OPTIONS`.

For example to instruct an ArcSight Console using IPV6 DNS entries, use the following commands:

on Unix

```
export ARCIGHT_JVM_NET_OPTIONS=
-Djava.net.preferIPv6Addresses=true
```

on Windows set

```
ARCIGHT_JVM_NET_OPTIONS=-Djava.net.preferIPv6Addresses=true
```

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

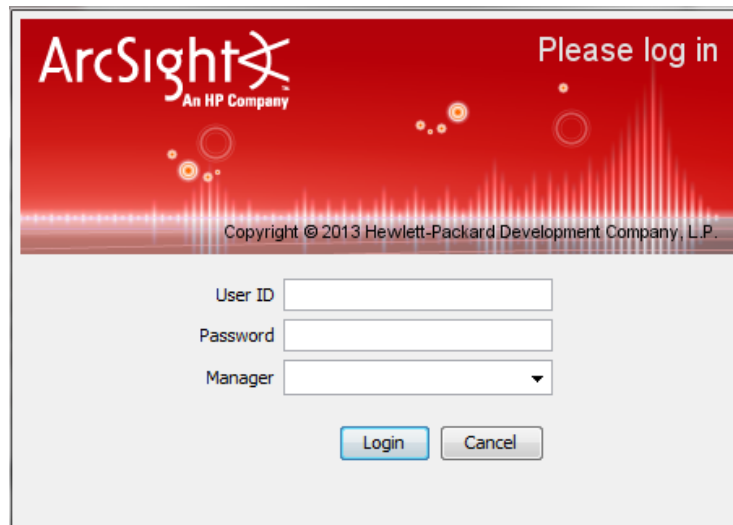
To start the ArcSight Console, use the shortcuts installed or open a command window on the Console's bin directory and run:

### 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 Cancel
Password Based and SSL Client Based Authentication	Login 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



Note

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 6.5c Console ->Uninstall ArcSight ESM Console 6.5c**

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

`ArcSight_ESM_Console_6.5c.exe`

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

`./ArcSight_ESM_Console_6.5c`



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).

---

## 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 53](#)  
["Customizing ESM Components Further" on page 55](#)  
["Fatal Error when Running the First Boot Wizard" on page 56](#)  
["Changing the Host Name of the Machine After Running the First Boot Wizard" on page 58](#)

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
First Boot Wizard Logs		
fbwizard.log	/opt/arcsight/manager/logs/default/	Contains detailed troubleshooting information logged during the steps in <a href="#">"Configuration" on page 25</a> .
firstbootsetup.log	/opt/arcsight/manager/logs/	Contains brief troubleshooting information about commands that ran during the steps in <a href="#">"Configuration" on page 25</a> .
CORR-Engine Log Files		

Log file name	location	Description
logger_server.log	/opt/arcsight/logger/current/arcsight/logger/logs	Contains troubleshooting information about the CORR-Engine
logger_server.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engine stdout log file
arcsight_logger.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_init_driver.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_init.sh.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_wizard.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_wizard.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
<b>Manager Log Files</b>		
server.log	/opt/arcsight/manager/logs/default	Contains troubleshooting information about the Manager
server.std.log	/opt/arcsight/manager/logs/default	Contains the stdout output of the Manager
server.status.log	/opt/arcsight/manager/logs/default	Contains a dump of all the MBeans, the memory status, thread status, etc.
<b>ArcSight Web Log Files</b>		
webserver.log	/opt/arcsight/web/logs/default	Contains troubleshooting information about ArcSight Web
webserver.std.log	/opt/arcsight/web/logs/default	Contains the stdout output of ArcSight Web
server.status.log	/opt/arcsight/web/logs/default	Manager status monitoring log file
<b>Log file for services</b>		
arcsight_services.log	/opt/arcsight/services/logs/	Contains information from commands that manage ArcSight service processes.

Log file name	location	Description
monit.log	/opt/arcsight/services/monit/data/	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 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 53](#).

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 18](#) 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 34](#) 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

If you have configured peering, make sure to re-establish the peer relationship.

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



Note

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

```
/sbin/service arcsight_services start arcsight_web
```
- 11 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.
- 12 Test to make sure that

- ◆ the clients can connect to the Manager
- ◆ peer configuration works as expected. If not, redo the peer configuration.

## 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 61](#)

[“CORR-Engine” on page 61](#)

[“Manager” on page 62](#)

[“ArcSight Web” on page 63](#)

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	changeit
default password for cacerts	changeit
default password for keystore	password

## 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	/opt/arcsight/logger
Database user name	arcsight
Database Port	3306

# Manager



The 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 the Manager for you:

Setting	Default Value
Location of Manager	/opt/arcsight/manager
Manager host name	Host name or IP address of ESM
Manager Port	8443
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	password
Default password for cacerts	changeit
Default password for truststore	changeit
Default password for nssdb and nssdb.client (both used in FIPS mode)	changeit
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>):  <pre>/sbin/service arcsight_services stop manager</pre> </li> <li>2 Run the following command from the /opt/arcsight/manager/bin directory and set up the external SMTP server when prompted:  <pre>./arcsight managersetup</pre> </li> <li>3 Start the Manager by running (as user <i>arcsight</i>):  <pre>/sbin/service arcsight_services start manager</pre> </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	/opt/arcsight/web
ArcSight Web host name	Host name or IP address of ESM
ArcSight Web Port	9443
Java Heap Memory	1 GB
Authentication Type	Password Based
Type of certificate used	self-signed
Default password for keystore	password
Default password for cacerts	changeit
Default password for truststore	changeit
Default password for nssdb	changeit





## Appendix C

# Using the PKCS#11 Token

---

This appendix covers the following topics:

- ["What is PKCS?" on page 65](#)
- ["PKCS#11 Token Support in ESM" on page 66](#)
- ["References to <ARCSIGHT\\_HOME>" on page 66](#)
- ["Setting Up to Use a CAC Card" on page 66](#)
- ["Logging in to the ArcSight Command Center Using CAC" on page 74](#)
- ["Using CAC with ArcSight Web" on page 75](#)

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 of 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 ArcSight 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 Command Center.
- 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 ArcSight 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 ArcSight 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 Command Center, 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 ArcSight 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 Command Center. Refer to your CAC provider's documentation on how to install and configure it.



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.

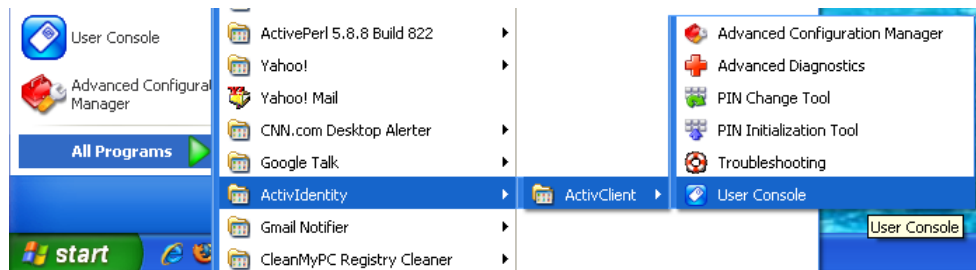
## Map a User's External ID to the CAC's Subject CN

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

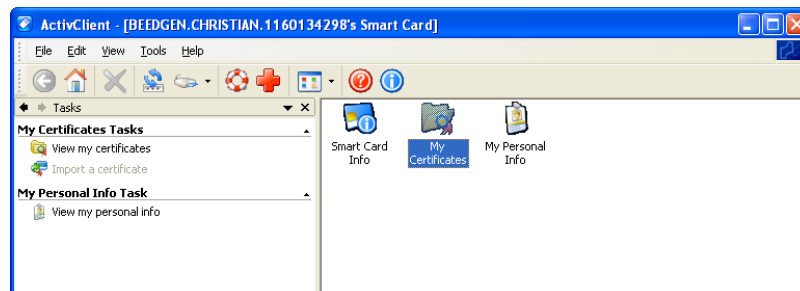
Map the Common Name (CN) on the CAC to a User's External ID on the ArcSight Manager. The external user ID must be identical to the Common Name that appears in the CAC card's ID certificate (include any spaces and periods that appear in the Common name). This allows the ArcSight Manager to know which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

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

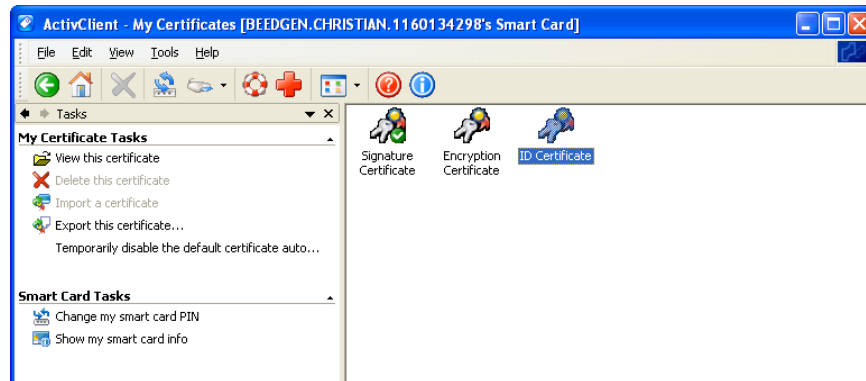
- 1 Obtain the Subject CN from the CAC card.
  - a Insert the CAC card into the reader if not already inserted.
  - b Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



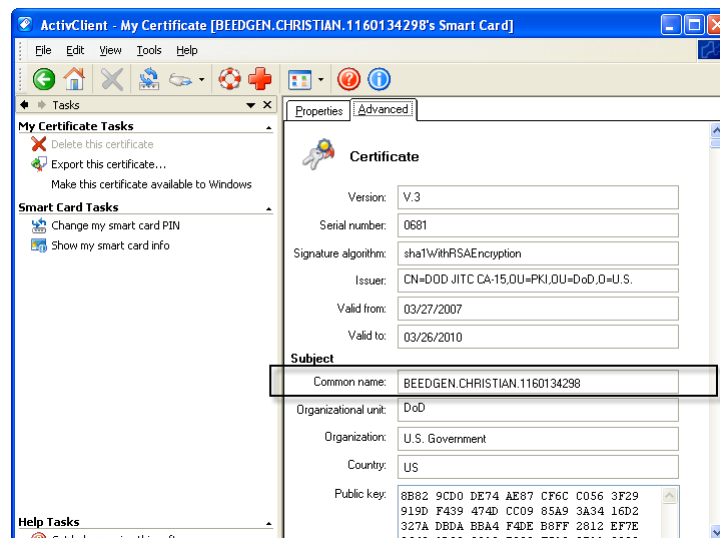
- c Double-click **My Certificates** in the following screen:



- 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 Command Center, 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:

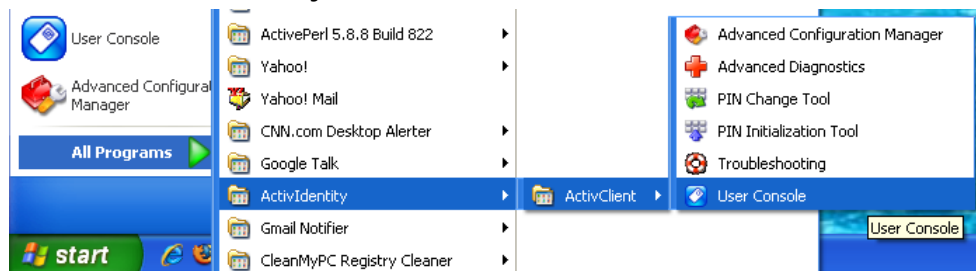
You can obtain the CAC card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

### Option 2:

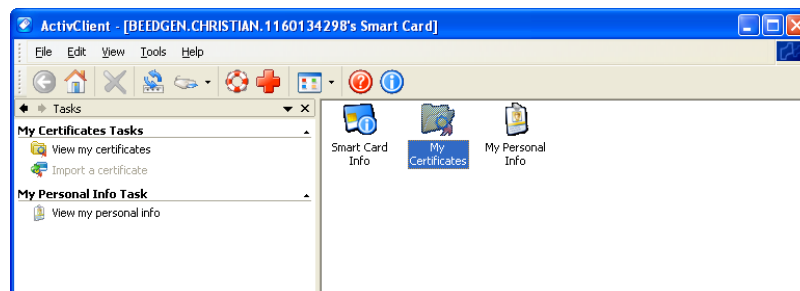
You can export the CAC card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

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

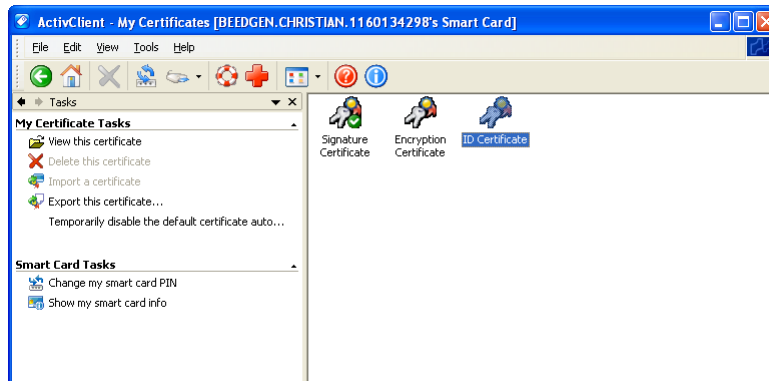
- 1 Insert the CAC card into the reader if not already inserted.
- 2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



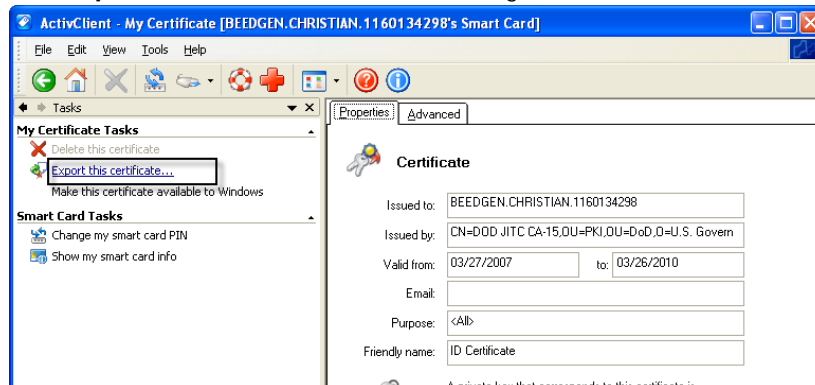
- 3 Double click **My Certificates** in the following screen:



- 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.

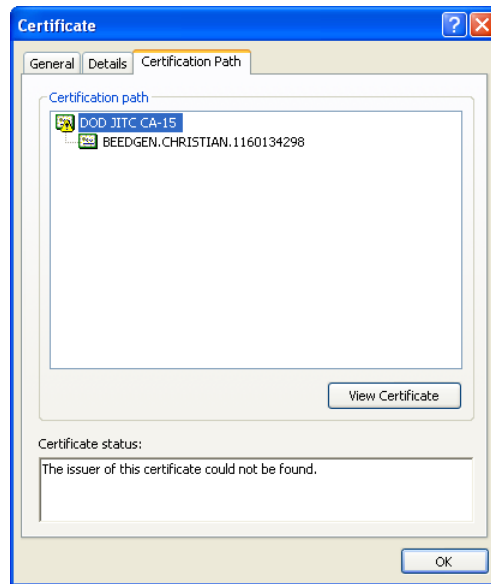
## Extract the Root CA Certificate From the CAC Certificate

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

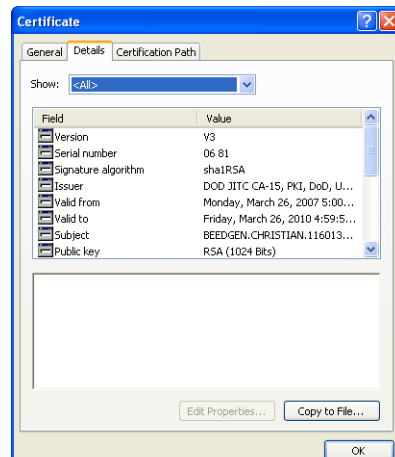
You should extract all intermediate certificates too (if any exist) using the following steps:

- 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 ArcSight Manager

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

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

To import the certificate into the ArcSight Manager's nssdb:

- 1 Stop the ArcSight Manager while logged in 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 ArcSight Manager while logged in as user "arcsight" by running:

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

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

Use the following procedure to import the CAC card's root CA certificate into the ArcSight 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 ArcSight Manager while logged in as user "arcsight" by running:

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

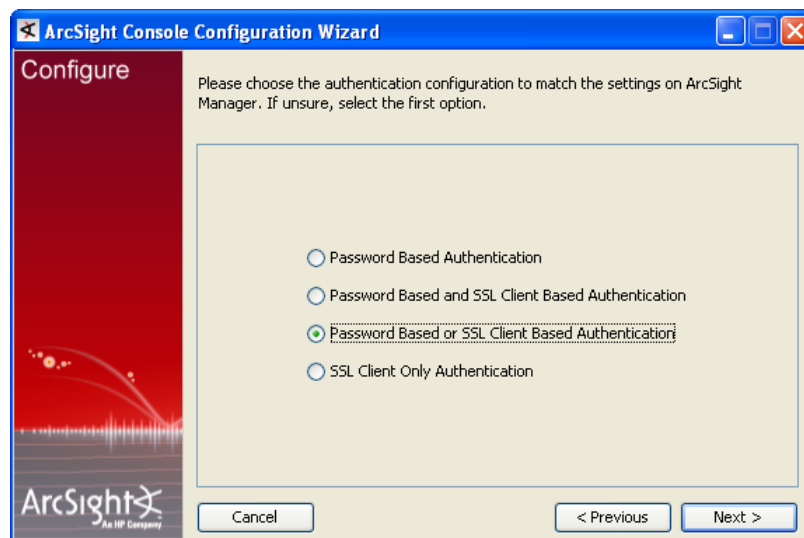


## Select Authentication Option in ArcSight Console Setup

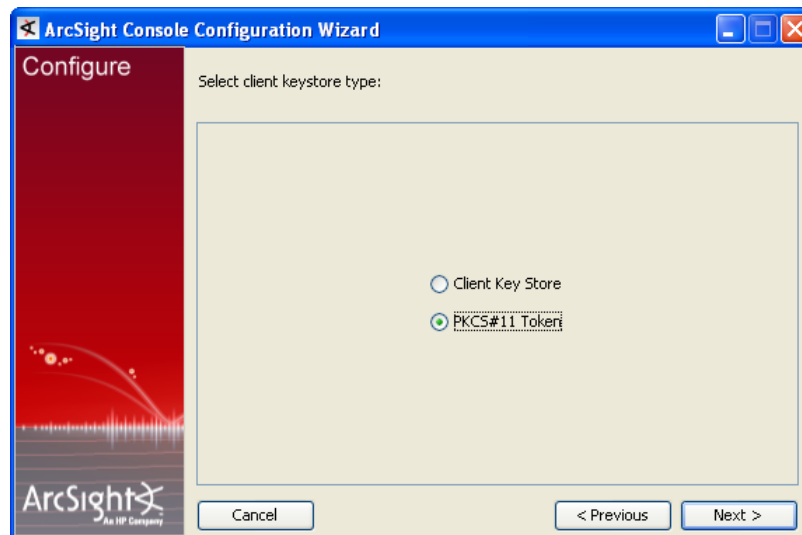
The authentication option on the ArcSight Console should match the authentication option that you set on the ArcSight Manager. Run the ArcSight Console setup program and either confirm or change the authentication on the ArcSight Console to match that of the ArcSight Manager. To do so:

- 1 Stop the ArcSight Console if it is running.
- 2 Run the ArcSight Console's setup program from the ArcSight 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 ArcSight 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.

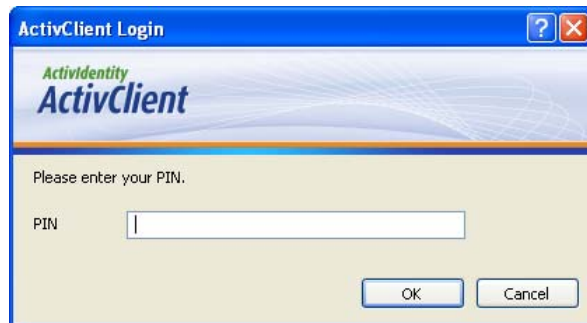
## Logging in to the ArcSight Console Using CAC

When you start the ArcSight 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.

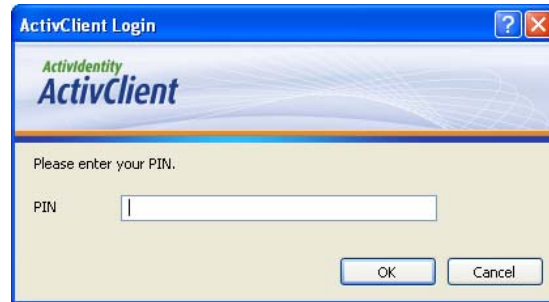


## Logging in to the ArcSight Command Center Using CAC

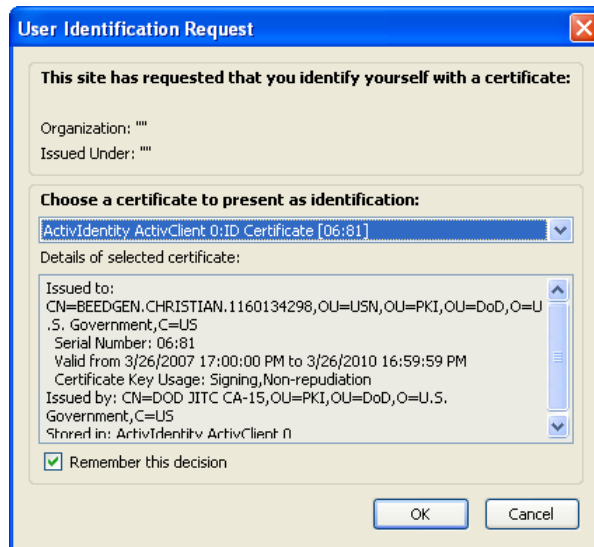
Use a supported web browser such as Firefox or Internet Explorer to connect to the ArcSight Command Center.

- 1 Make sure that the CAC card is securely placed in its card reader.
- 2 Go to this web site: <https://<hostname>:8443/>.

- 3 You will be requested to enter your PIN



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



- 4 At the ArcSight Command Center 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 ArcSight Command Center. When the ArcSight Command Center is set up for CAC, no additional setup is required to access ArcSight Web, because its CAC access is handled by the ArcSight Command Center.



## Appendix D

# ESM in FIPS Mode

---

This section covers the following topics:

- [“What is FIPS?” on page 77](#)
- [“Network Security Services Database \(NSS DB\)” on page 78](#)
- [“What is Suite B?” on page 78](#)
- [“NSS Tools Used to Configure Components in FIPS Mode” on page 79](#)
- [“TLS Configuration in a Nutshell” on page 79](#)
- [“Using PKCS #11 Token With a FIPS Mode Setup” on page 81](#)
- [“Installing ArcSight Console in FIPS Mode” on page 82](#)
- [“Configure Your Browser for FIPS” on page 86](#)
- [“Installing SmartConnectors in FIPS mode” on page 88](#)
- [“How do I Know If My Installation is FIPS Enabled?” on page 89](#)

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 ArcSight 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 an ArcSight 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. We recommend 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 ArcSight 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 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 ArcSight 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.
- `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:

On Windows:

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

On Linux:

```
./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 ArcSight Manager, ArcSight 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 (ArcSight Manager) authenticates itself to the client (ArcSight Console, ArcSight Web). This is called server side authentication. To set up TLS configuration on your ArcSight Manager for server side authentication, you need:

- A key pair in your ArcSight Manager's NSS DB.
- The ArcSight Manager's certificate, which incorporates the public key from the key pair located in the ArcSight Manager's NSS DB. By default, this is a self-signed certificate.

Next, you should export the ArcSight 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 ArcSight 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 (ArcSight Manager) has authenticated itself to the client (ArcSight Console or ArcSight Web). At this point, the server requests the client to authenticate itself.

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

- A key pair.
- The ArcSight Console's certificate, which incorporates the ArcSight 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 ArcSight Manager's NSS DB as the token is a client to the ArcSight Manager.

For detailed procedures on each of the steps mentioned above, refer to ["Setting up Client-Side Authentication" on page 212](#) 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 ArcSight 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 ArcSight Manager but has to authenticate itself to web browsers.

To authenticate the ArcSight Manager, it should have the ArcSight 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 ArcSight Manager's certificate for Other Clients

You are required to have this exported certificate available when installing clients that connect to this ArcSight 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 ArcSight Manager's certificate allows the clients to trust the ArcSight Manager.

To export the ArcSight Manager's certificate, run the following command from the ArcSight 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 ArcSight 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 ArcSight 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 ArcSight Manager's certificate, in the `/opt/arcsight/manager` directory.

## References to ARCSIGHT\_HOME

`<ARCSIGHT_HOME>` in the paths represents:

- `/opt/arcsight/manager` for the ArcSight 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 65](#).

- 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 Command Center. See ["Install the CAC Provider's Software" on page 66](#).
- 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 ArcSight Manager's nssdb.

## Installing ArcSight Console in FIPS Mode



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

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

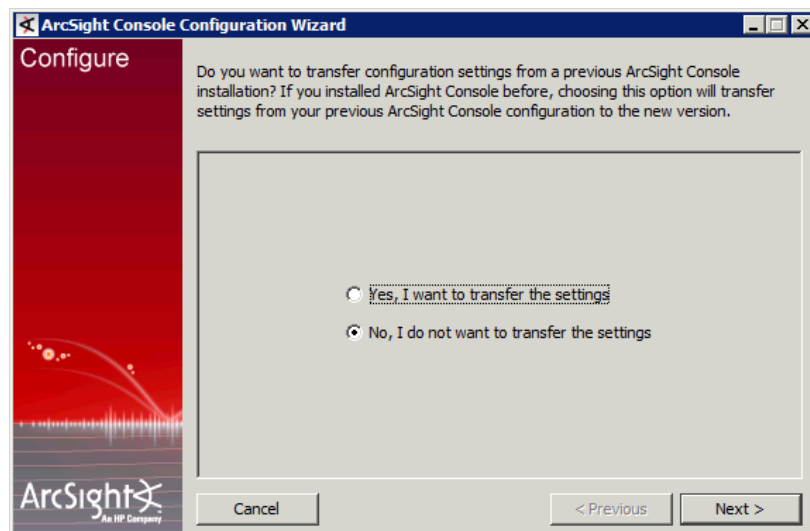
Refer to the ESM Product Lifecycle document available on the Protect 724 website (<https://protect724.arcsight.com>) for details on supported platforms for the ArcSight Console.

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

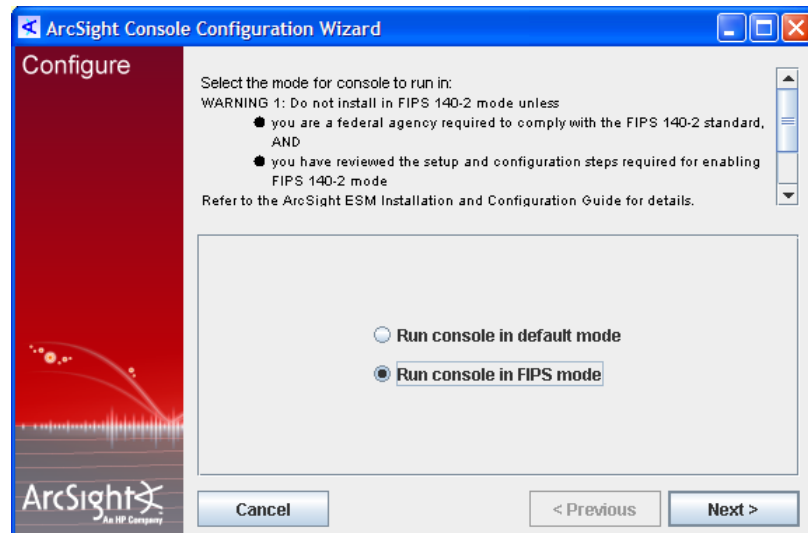
In order for an ArcSight Console to communicate with a FIPS enabled ArcSight Manager, the ArcSight Console must trust the ArcSight Manager. This trust is established by importing the ArcSight Manager's certificate into the ArcSight Console's NSS DB (<ARCSIGHT\_HOME>/current/config/nssdb.client). After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

To install the ArcSight 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**.

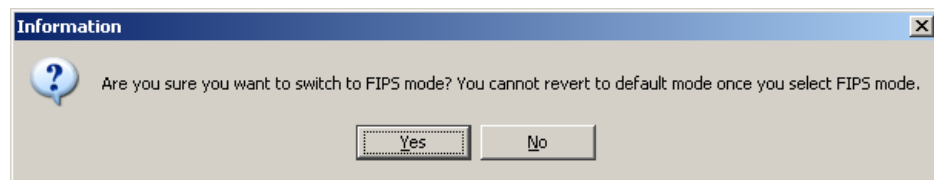


- 4 Next, you will see the following screen:



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

- 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**.

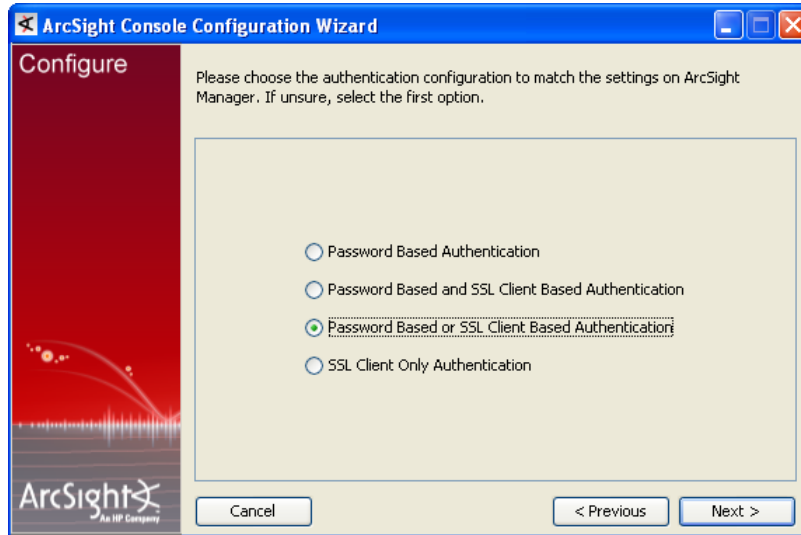


- 6 You will be prompted to select a cipher suite. Select the type of FIPS the ArcSight Manager uses and click **Next**.



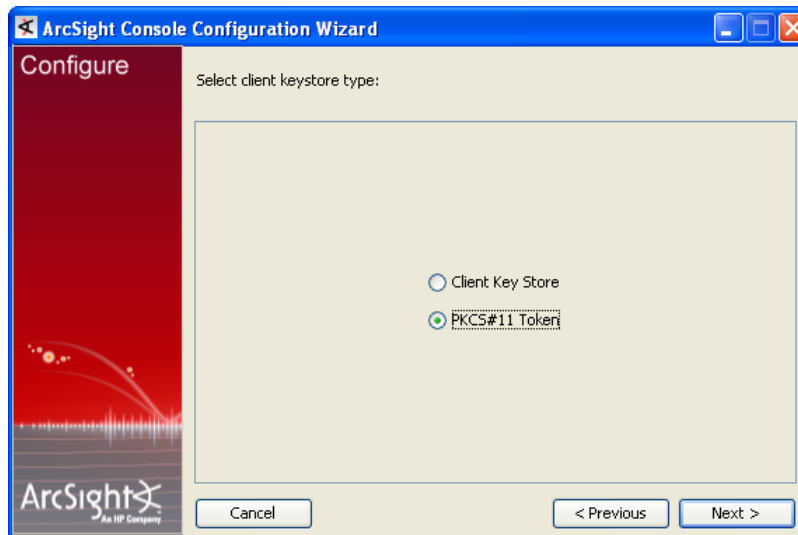
- 7 Next you will be prompted for the ArcSight Manager's hostname and port. The ArcSight Manager hostname must be the same (short name, fully qualified domain name, or IP address) as the Common Name (CN) you used when you created the ArcSight Manager key pair.

- 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 ArcSight 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 ArcSight Console, select **PKCS #11 Token** option in the following screen. Otherwise skip this step.



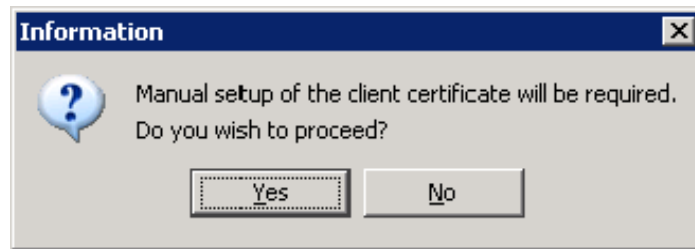
Enter the path or browse to the PKCS #11 library.

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

On 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 ArcSight 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 F, Configuration Changes Related to FIPS](#), on [page 197](#), in the Administrator's Guide to set up the client certificate.

- 10 Follow the prompts in the next few wizard screens to complete the ArcSight 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 ArcSight Console on Windows. You cannot use the Internet Explorer browser because it does not support FIPS with Suite B.

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

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

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

- Either add `server.fips.enabled=true` in your `console.properties` file located in the ArcSight Console's `<ARCSIGHT_HOME>/current/config` directory.  
Or add `-Dhttps.protocols=TLSv1` to the `ARCSIGHT_JVM_OPTIONS` variable in the ArcSight Console's `<ARCSIGHT_HOME>/current/bin/scripts/console.sh` file.
- Import the ArcSight Manager's certificate into `<ARCSIGHT_HOME>/current/jre/lib/security/cacerts` on the ArcSight 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 ArcSight Console running in Default mode to connect to a FIPS enabled ArcSight Manager by following the steps above, you will not be able to connect this ArcSight Console to a ArcSight Manager running in Default mode without reversing the changes you made to the files.



Note

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

## Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers

This procedure should be automatic for multiple ArcSight Managers. Just make sure that each ArcSight 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 ArcSight Console's `nssdb.client`.

If you need to import a ArcSight Manager's certificate into the ArcSight 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 ArcSight Command Center.

### FIPS with Firefox

FIPS can be configured for versions of Firefox up to version 17 ESR. The steps for Firefox are more involved than for other browsers, so they are included here.

- 1 In the Firefox window, select **Tools->Options...** (or **Edit->Preferences** in the case of Firefox on Linux)
- 2 In the Options window, click the **Advanced** icon.
- 3 Click the **Encryptions** tab to open the page.
- 4 Uncheck the **Use SSL 3.0** check box.
- 5 Check the **Use TLS 1.0** check box.
- 6 Click the **Security Devices** button to open the Device Manager dialog where you will enable FIPS in Firefox's NSS internal PKCS #11 module.
- 7 Click **Software Security Device** and click **Change Password** button.
- 8 Enter a new password and re-enter it to confirm it.
- 9 Select **NSS Internal PKCS #11 Module** and click **Enable FIPS** button.
- 10 Click **OK** to close the Device Manager window and click **OK** to close the Preferences window.
- 11 You must disable all non-FIPS TLS cipher suites. In the location box of the Firefox browser, enter `about:config` and press **Enter**.
- 12 In the message that follows, click the **I'll be careful, I promise** button.
- 13 In the **Filter** textbox, type `ssl`.
- 14 Compare the true/false value for each preference listed on the page that follows with the preference Value in the screenshot below and make sure that the true/false value

match the ones shown in the screenshot below. If any preference value does not match, double click its value to toggle it.

Preference Name	Status	Type	Value
security.enable_ssl2	default	boolean	false
<b>security.enable_ssl3</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl2.des_64	default	boolean	false
security.ssl2.des_ede3_192	default	boolean	false
security.ssl2.rc2_128	default	boolean	false
security.ssl2.rc2_40	default	boolean	false
security.ssl2.rc4_128	default	boolean	false
security.ssl2.rc4_40	default	boolean	false
security.ssl3.dhe_dss_aes_128_sha	default	boolean	true
security.ssl3.dhe_dss_aes_256_sha	default	boolean	true
<b>security.ssl3.dhe_dss_camellia_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
<b>security.ssl3.dhe_dss_camellia_256_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.dhe_dss_des_ede3_sha	default	boolean	true
security.ssl3.dhe_dss_des_sha	default	boolean	false
security.ssl3.dhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.dhe_rsa_aes_256_sha	default	boolean	true
<b>security.ssl3.dhe_rsa_camellia_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
<b>security.ssl3.dhe_rsa_camellia_256_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.dhe_rsa_des_ede3_sha	default	boolean	true
security.ssl3.dhe_rsa_des_sha	default	boolean	false
security.ssl3.ecdh_ecdsa_aes_128_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_aes_256_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_null_sha	default	boolean	false
<b>security.ssl3.ecdh_ecdsa_rc4_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.ecdh_rsa_aes_128_sha	default	boolean	true
security.ssl3.ecdh_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdh_rsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdh_rsa_null_sha	default	boolean	false
<b>security.ssl3.ecdh_rsa_rc4_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.ecdhe_ecdsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_null_sha	default	boolean	false
<b>security.ssl3.ecdhe_ecdsa_rc4_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.ecdhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_rsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdhe_rsa_null_sha	default	boolean	false
<b>security.ssl3.ecdhe_rsa_rc4_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.rsa_1024_des_cbc_sha	default	boolean	false
security.ssl3.rsa_1024_rc4_56_sha	default	boolean	false
security.ssl3.rsa_aes_128_sha	default	boolean	true
security.ssl3.rsa_aes_256_sha	default	boolean	true
<b>security.ssl3.rsa_camellia_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
<b>security.ssl3.rsa_camellia_256_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.rsa_des_ede3_sha	default	boolean	true
security.ssl3.rsa_des_sha	default	boolean	false
<b>security.ssl3.rsa_fips_des_ede3_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.rsa_fips_des_sha	default	boolean	false
security.ssl3.rsa_null_md5	default	boolean	false
security.ssl3.rsa_null_sha	default	boolean	false
security.ssl3.rsa_rc2_40_md5	default	boolean	false
<b>security.ssl3.rsa_rc4_128_md5</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
<b>security.ssl3.rsa_rc4_128_sha</b>	<b>user set</b>	<b>boolean</b>	<b>false</b>
security.ssl3.rsa_rc4_40_md5	default	boolean	false

**15** In addition, change the preference `network.http.spdy.enabled` to false.

**16** Disable the TLS Ticket Extension as follows:

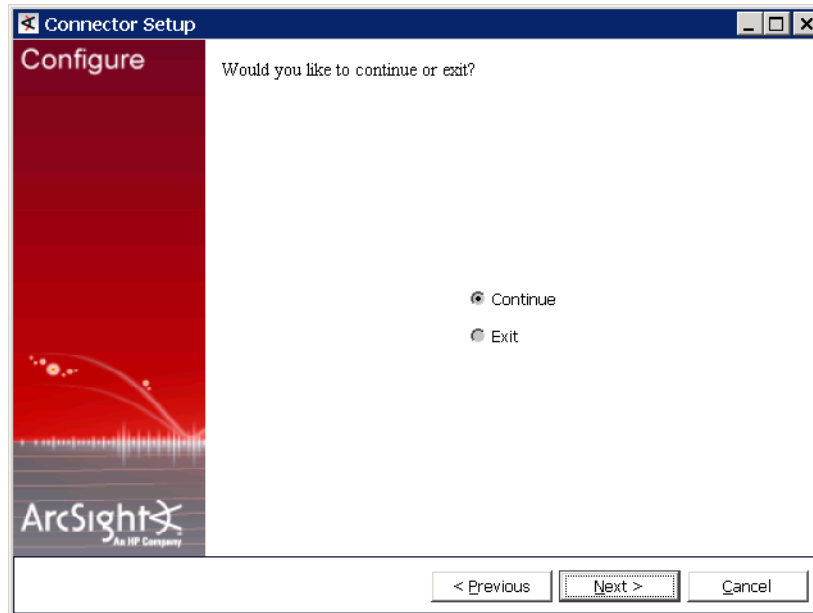
- a** In the Filter textbox, enter TLS.
- b** Change the value of `security.enable_tls_session_tickets` preference to false by double-clicking it.



- c Quit the browser and restart it; then connect to the webserver.

## Installing SmartConnectors in FIPS mode

When the ArcSight 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 **Continue** and click **Next**.



Use the following procedure to continue:

- 1 After choosing **Continue** and clicking **Next** after connector installation, choose **Enable FIPS Mode** and click **Next**. A confirmation window is displayed when FIPS mode is enabled.
- 2 Click **Next**. To complete installation of FIPS support, click **Exit**. To enable FIPS Suite B mode, click **Continue**.
- 3 On the window displayed, select **Modify Connector**.
- 4 Select **Add, Modify, or remove destinations** and click **Next**.
- 5 Select the destination for which you want to enable FIPS Suite B mode and click **Next**.
- 6 Select **Modify destination parameters** and click **Next**.
- 7 When the parameter window is displayed, select **FIPS with Suite B 128 bits** or **FIPS with Suite B 192 bits** for the **FIPS Cipher Suites** parameter. Click **Next**.
- 8 The window displayed shows the editing changes to be made. Confirm and click **Next** to continue. (To adjust changes before confirming, click **Previous**.)
- 9 A summary of the configuration changes made is displayed. Click **Next** to continue.
- 10 Click **Exit** to exit the configuration wizard.

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 ArcSight Manager
- `<ARCSIGHT_HOME>/current/config/console.properties` for the ArcSight Console
- `/opt/arcsight/web/config/webserver.properties` for ArcSight Web
- `<ARCSIGHT_HOME>/user/agent/agent.properties` for the Partition Archiver.

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

- Administrator user 14
- appendix
  - example of 65, 77
- ArcSight
  - Manager 7
- ArcSight Console
  - client authentication 44
  - connecting to the Manager 41
  - installing 37, 38
  - reconfiguring 52
  - reconnecting to Manager 51
  - starting 49
  - uninstalling 52
  - user logs and preferences 46
  - web browser configuration 45
- ArcSight Manager
  - default settings 62
- ArcSight Web 13
  - overview 8

## C

- changing
  - host name 58
  - IP address 56
- character set 48
- client authentication
  - ArcSight Console 44
- configuration
  - web browser in Console 45
- connecting
  - ArcSight Console to Manager 41
- Console
  - installing 38
  - supported platforms 37
- customizing
  - components 55

## D

- default settings
  - ArcSight Manager 62
- Deployment Overview 9
- directory structure
  - ArcSight Installation 11

## E

- ESM 7
  - built-in security 13
  - components 7

- effects of communication when components fail 9
- overview 7
- securing 12

## F

- First Boot Wizard
  - fatal error 56

## G

- guidelines
  - security 14

## H

- hardware
  - security 13
- host name, changing 58
- hot key issue 48

## I

- installing
  - ArcSight Console 38
  - directory structure 11
- IP address, changing 56

## M

- Manager 7
  - ports 12
  - protecting 12
  - select packages 31
  - transferring configuration 40

## O

- operating system
  - security 14

## P

- passwords
  - character set 48
- preferences
  - ArcSight Console 46

## R

- reconfiguring
  - ArcSight Console 52
- reconnecting

- Console to Manager 51
- restarting
  - First boot wizard 34

## S

- security 13
  - guidelines and policies 14
  - hardware 13
  - operating system 14
- shortcut key issue 48
- starting
  - ArcSight Console 49
- supported platforms
  - Console 37

## T

- Troubleshooting 53
  - fatal error 56

## U

- uninstalling
  - ArcSight Console 52
- user logs
  - ArcSight Console 46

## W

- Web 8
- Web browser
  - configuring in Console 45
- wizard
  - restarting 34