

# Configuration Guide

---

ArcSight Express 4.0  
with CORR-Engine

April 1, 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#.URitMaVwpWI">http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI</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
04/01/2013	ArcSight Express 4.0	Configuring ArcSight Express and the components that reside on it

# Contents

---

<b>Chapter 1: What is ArcSight Express?</b>	<b>7</b>
Pre-installed Components on ArcSight Express	7
ArcSight Manager	8
CORR-Engine	8
Connector Management	8
ArcSight SmartConnectors	8
ArcSight Console	8
Deployment Overview	9
ArcSight Express Communication Overview	9
Effect on Communication when Components Fail	10
Choosing between FIPS Mode or Default Mode	11
Differences Between Default Mode, FIPS Mode, and FIPS with Suite B Mode	11
Using PKCS#11	11
Import Control Issues	12
<b>Chapter 2: Configuring the ArcSight Express Appliance</b>	<b>13</b>
Before You Configure the Appliance	13
Configuring the ArcSight Express Appliance	13
The First Boot Wizard	14
Post Configuration Steps	23
Setting Up SmartConnectors	24
Setting Up Client-Side Authentication on SmartConnectors	25
To Set Up ArcSight Express in a Non English Environment	25
On the ArcSight Manager	25
On the ArcSight Console	25
The Next Steps	26
<b>Chapter 3: Running the ArcSight Manager Configuration Wizard</b>	<b>27</b>
Running the Wizard	27
Authentication Details	32
How external authentication works	32
Guidelines for setting up external authentication	32
Password Based Authentication	33
Password Based and SSL Client Based Authentication	36

Password Based or SSL Client Based Authentication .....	36
SSL Client Only Authentication .....	36
<b>Chapter 4: Installing ArcSight Console .....</b>	<b>37</b>
ArcSight Console Supported Platforms .....	37
Required Libraries on the RHEL 6.2 64 Bit Workstation .....	37
Using a PKCS#11 Token .....	38
Installing the ArcSight Console .....	39
Character Set Encoding .....	40
Configuration Settings .....	41
Selecting the Mode in which to Configure ArcSight Console .....	41
ArcSight Manager Connection .....	42
Authentication .....	45
Web Browser .....	47
Importing the ArcSight Console's Certificate into the Browser .....	50
Starting the ArcSight Console .....	50
Logging into the ArcSight Console .....	52
Reconnecting to the ArcSight Manager .....	52
Reconfiguring the ArcSight Console .....	53
Uninstalling the ArcSight Console .....	53
<b>Chapter 5: Using SmartConnectors .....</b>	<b>55</b>
Installing SmartConnectors .....	55
ArcSight SmartConnectors with ArcSight Express .....	56
First Boot Wizard Configuration .....	56
About Pre-Bundled Connectors .....	57
The Microsoft Windows Event Log - Unified SmartConnector .....	57
The Syslog Daemon SmartConnector .....	57
Set Up Pre-Bundled Connector Devices .....	58
Syslog .....	58
Microsoft Windows Event Log - Unified .....	59
General Information .....	60
Authentication .....	60
ArcSight Services .....	60
FIPS Support .....	60
FIPS Compliant Connectors .....	60
Non-FIPS Compliant Connectors .....	60
Caveats .....	61
Connector Upgrade .....	61
Add Connectors .....	61
Model Import Connector for RepSM .....	61
ESM Forwarding Connector .....	62
Update Connector Parameters .....	62

Importing the Manager's Certificate .....	62
Using keytoolgui to Import Manager's Certificate .....	63
Exporting the Manager's Certificate .....	63
Importing the Manager's Certificate into the SmartConnector's Truststore .....	65
<b>Appendix A: Troubleshooting .....</b>	<b>69</b>
Location of Log files for Components .....	69
Customizing ArcSight Express Components Further .....	71
Fatal Error When Running the First Boot Wizard .....	72
Changing the IP Address of Your Machine .....	73
Changing the Host Name of the Machine After Running the First Boot Wizard .....	74
The remote_management.p12 file is empty .....	76
<b>Appendix B: Default Settings for Components .....</b>	<b>77</b>
General .....	77
CORR-Engine .....	77
ArcSight Manager .....	78
ArcSight Web .....	79
SmartConnectors .....	79
<b>Appendix C: About Locales and Encodings .....</b>	<b>81</b>
Terminology .....	81
Internationalization .....	81
Locale .....	81
Character Set .....	81
Code Set .....	81
Code Point .....	82
Encoding .....	82
Unicode .....	82
Before you Install a Localized Version of ArcSight Express .....	82
ArcSight Console .....	83
ArcSight SmartConnectors .....	83
Setting the Encoding for Selected SmartConnectors .....	83
Localization of Date Formats in Tokens and Operations .....	84
Key-Value Parsers for Localized Devices .....	84
Examples .....	85
Scenario 1 - Events received in a single language only .....	85
First Boot Wizard .....	85
ArcSight Manager, ArcSight Console, and ArcSight Web .....	85
Scenario 2 - Events received in multiple languages .....	85
First Boot Wizard .....	85
ArcSight Manager, ArcSight Console, and ArcSight Web .....	85
List of possible values for the agent.parser.locale.name property .....	85

<b>Appendix D: Using the PKCS#11 Token .....</b>	<b>91</b>
What is PKCS? .....	91
PKCS#11 .....	91
PKCS#12 .....	91
PKCS#11 Token Support in ArcSight Express .....	92
References to <ARCSIGHT_HOME> .....	92
Setting Up to Use a CAC Card .....	92
Install the CAC Provider's Software .....	92
Map a User's External ID to the CAC's Subject CN .....	93
Obtain the CAC's Issuers' Certificate .....	95
Extract the Root CA Certificate From the CAC Certificate .....	96
Import the CAC Root CA Certificate into the ArcSight Manager .....	97
FIPS Mode - Import into the ArcSight Manager's nssdb .....	98
Default Mode - Import into the ArcSight Manager's Truststore .....	98
Select Authentication Option in ArcSight Console Setup .....	99
Logging in to the ArcSight Console Using CAC .....	100
Logging in to the Management Console Using CAC .....	100
Using CAC with ArcSight Web .....	101
<b>Appendix E: ArcSight Express in FIPS Mode .....</b>	<b>103</b>
What is FIPS? .....	103
Network Security Services Database (NSS DB) .....	104
What is Suite B? .....	104
NSS Tools Used to Configure Components in FIPS Mode .....	105
TLS Configuration in a Nutshell .....	105
Understanding Server Side Authentication .....	106
Understanding Client Side Authentication .....	106
Setting up Authentication on ArcSight Web - A Special Case .....	106
Exporting the ArcSight Manager's certificate for Other Clients .....	107
References to ARCSIGHT_HOME .....	107
Using PKCS #11 Token With a FIPS Mode Setup .....	107
Installing ArcSight Console in FIPS Mode .....	108
Connecting a Default Mode ArcSight Console to a FIPS 140-2 ArcSight Manager .....	112
Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers .....	112
Configure Your Browser for FIPS .....	112
FIPS with Firefox .....	112
Installing SmartConnectors in FIPS mode .....	115
How do I Know If My Installation is FIPS Enabled? .....	116
<b>Appendix F: Restoring Factory Settings .....</b>	<b>117</b>
<b>Index .....</b>	<b>119</b>

# Chapter 1

## What is ArcSight Express?

---

The ArcSight Express appliance 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 that are of interest to you.

ArcSight Express 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.

ArcSight Express uses the Correlation Optimized Retention and Retrieval Engine Storage (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 and more compact data storage.

This chapter covers the following topics:

[“Pre-installed Components on ArcSight Express” on page 7](#)

[“ArcSight SmartConnectors” on page 8](#)

[“ArcSight Console” on page 8](#)

[“Deployment Overview” on page 9](#)

[“ArcSight Express Communication Overview” on page 9](#)

## Pre-installed Components on ArcSight Express

The ArcSight Express appliance has the following software components pre-installed on it:

- ArcSight Manager
- CORR-Engine
- Pre-bundled connectors - Syslog Daemon SmartConnector and Microsoft Windows Event Log - Unified SmartConnector - these connectors are already installed on ArcSight Express. You have the option to configure these connectors when running the First Boot Wizard for a fresh installation.
- Connector Management module



In addition to the pre-installed components listed above, you can also find the binaries for the Forwarding Connector and the Reputation Security Monitor Model Import Connector on ArcSight Express. You can install these connectors after you have finished setting up the appliance.

---

## ArcSight Manager

ArcSight Manager is at the center of the ArcSight Express appliance. The ArcSight 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 ArcSight Manager also provides advanced correlation and reporting capabilities.

## CORR-Engine

ArcSight CORR-Engine is a long term data storage and retrieval engine that enables the product to receive events at high rates.

## Connector Management

The Connector Management tool allows for management of connectors that are pre-bundled on the appliance and remotely installed connectors using the Management Console. Pre-bundled connectors can be configured in the First Boot Wizard for a fresh installation. But if you did not configure them when running the First Boot Wizard, you have the option to configure them any time post installation using the Connector Management tab in the Management Console.

## ArcSight SmartConnectors

SmartConnectors are software components that send security events from a wide variety of devices and security event sources to the CORR-Engine. ArcSight Express bundles two SmartConnectors (Syslog Daemon SmartConnector and Windows Unified SmartConnector). Other connectors can be separately installed manually from the Connector Management module of the Management Console.

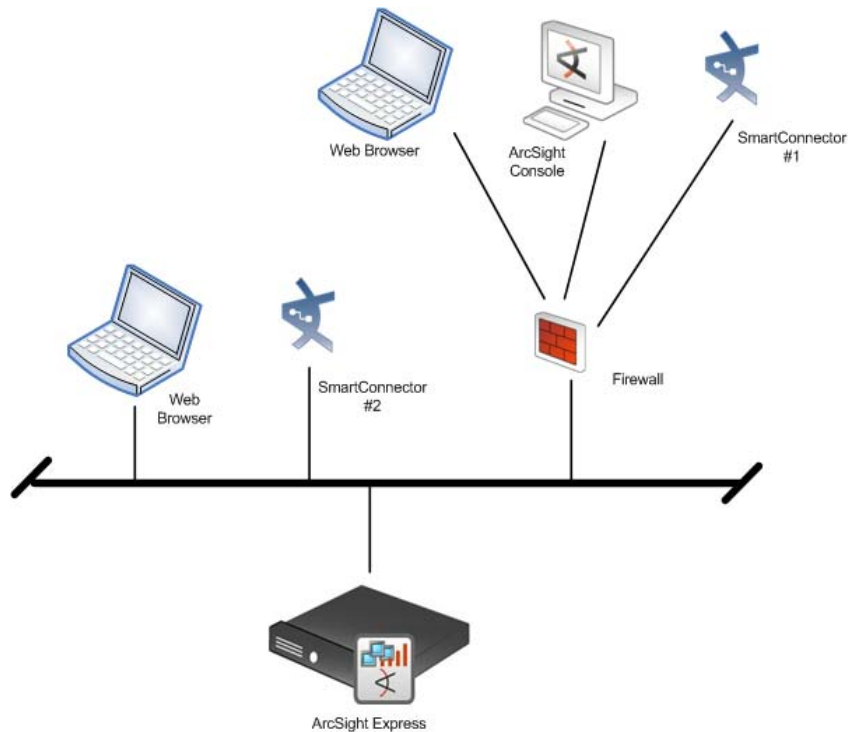
## ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks on ArcSight Express, such as fine tuning the pre-installed ArcSight Express content and managing users. The ArcSight Console is not bundled with ArcSight Express and should be separately installed on a system other than the ArcSight Express appliance.



## Deployment Overview

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

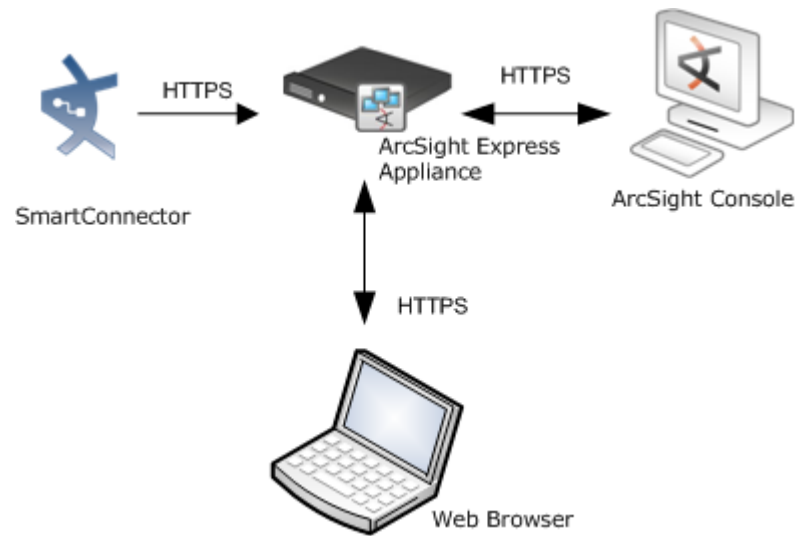


**Figure 1-1** ArcSight Express Deployment

## ArcSight Express Communication Overview

ArcSight Console, ArcSight Manager, and ArcSight SmartConnector communicate using HTTP (HyperText Transfer Protocol) over SSL (Secure Sockets Layer), often referred to as

HTTPS (HyperText Transfer Protocol Secure). The HTTPS protocol provides for data encryption, data integrity verification, and authentication for both server and client.



**Figure 1-2 ArcSight Express Solution - Communication**

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

The ArcSight Manager never makes outgoing connections to the ArcSight Console or SmartConnectors. The ArcSight Manager connects to the CORR-Engine on the appliance locally using JDBC.

## Effect on Communication when Components Fail

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

If the CORR-Engine is unavailable for any reason, the ArcSight 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 ArcSight Console gets disconnected.

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

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

ArcSight Express 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 following components in either of these modes:

- Default mode
- FIPS 140-2 mode

Before you install in FIPS mode, see [Appendix E, ArcSight Express in FIPS Mode, on page 103](#).

- FIPS with Suite B mode

Before you install in FIPS with Suite B mode, see [Appendix E, ArcSight Express in FIPS Mode, on page 103](#).

## Differences Between Default Mode, FIPS Mode, and FIPS with Suite B Mode

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

Mode	Use of SSL/TLS	Default Cipher Suites	Keystore/Truststore
Default Mode	SSL or 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> <li>More...</li> </ul>	Keypair and Certificates stored in Keystore 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

ArcSight Express supports the use of a PKCS#11 token such as the Common Access Card (CAC) to log into the ArcSight Console or ArcSight Web. PKCS#11 is Public-Key

Cryptography Standard (PKCS), published by RSA Laboratories which describes it as “a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.”

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

## Import Control Issues

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

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

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

They are available at:

`jre\lib\security\local_policy.jar.original`

`jre\lib\security\US_export_policy.jar.original`

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

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

## Chapter 2

# Configuring the ArcSight Express Appliance

---

This chapter covers the following topics:

- “Before You Configure the Appliance” on page 13
- “Configuring the ArcSight Express Appliance” on page 13
- “Setting Up Client-Side Authentication on SmartConnectors” on page 25
- “To Set Up ArcSight Express in a Non English Environment” on page 25
- “The Next Steps” on page 26

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

## Before You Configure the Appliance

Before you begin to configure the ArcSight Express appliance:

- Download the license zip file from the HP ArcSight Customer Support site, <http://support.openview.hp.com> on to the ArcSight Express appliance.



You do not need to unzip the license zip file. The ArcSight Express First Boot Wizard recognizes the license file in the zipped state.

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

## Configuring the ArcSight Express Appliance

The ArcSight Express appliance is configured using the First Boot Wizard which opens automatically when you boot the appliance for the very first time or when you boot the system after a factory restore.



Do not set up the pre-bundled connectors in this wizard if you plan to migrate your resources from Oracle to the CORR-Engine (from an older version of ArcSight Express appliance with Oracle). You can configure the connectors **after** you migrate the resources.

After you have stepped through the First Boot Wizard, follow the steps in the [Post Configuration Steps](#) section.

## The First Boot Wizard

The First Boot Wizard screens walk you through the process of setting up the preferences for the Red Hat Enterprise Linux operating system installed on the appliance as well as configuring the software components that have been pre-installed on the appliance.

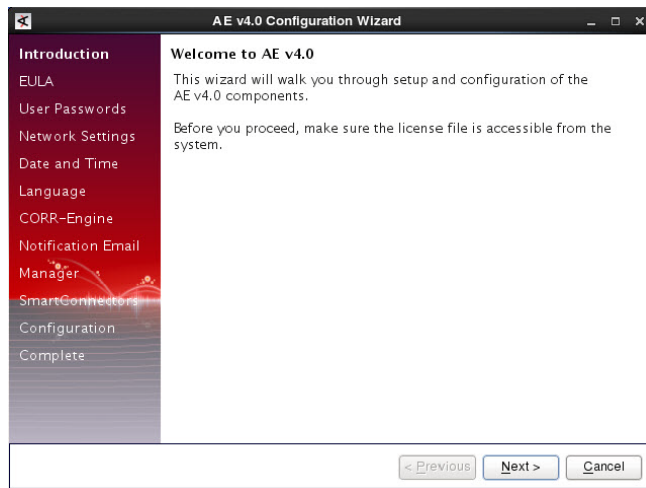
When the appliance first comes up, it automatically comes up logged in as the “root” user. The First Boot Wizard runs while logged in as the “root” user.



**Caution**

The settings that you change in the wizard are saved immediately when you click **Next**. So, if you cancel out of the wizard or you happen to reboot your appliance before the First Boot Wizard completes, log in as user root to relaunch the wizard.

- 1 Click **Next** on the Welcome screen.



- 2 Read the license agreement. This license agreement is for HP ArcSight EULA. At the very bottom of the agreement, select **I accept the License Agreement** if you agree with it, and click **Next**.
- 3 Enter and re-enter passwords to be set for the “root” account and the “arcsight” user account. The “root” account is used for system administration. For security reasons, the ArcSight Manager runs using an “arcsight” user account. The “arcsight” user account has already been created for you.

For information on password restrictions see the Administrator's Guide, chapter 2. “Configuration,” “Managing Password Configuration.” Click **Next**.

- 4 The next step is to configure the IP addresses for the appliance.

Enter the IP address, subnet mask, default gateway, primary and secondary DNS servers, and optional search domains for the ArcSight Express appliance.



Make sure that the IP address you set up is not already in use. The First Boot Wizard will report errors if the IP address has not been configured correctly.



If you want to change the hostname or IP address after you have finished running this wizard, follow the steps in the sections [“Changing the Host Name of the Machine After Running the First Boot Wizard”](#) on page 62 or [“Changing the IP Address of your machine”](#) on page 61 respectively.

Click **Next**. You will see a message asking you to confirm the settings. If you would like to use DHCP, for example, click No in the message box and then click **Next**.

- 5 In the **Date and Time** panel, you can either explicitly set the date and time or you can optionally specify one or more NTP servers from which the time gets synchronized. You have the option to retain the default NTP servers or add your own NTP server to the default list. This will configure the operating system to use the NTP servers specified in the list from which to obtain the time.

Click **Next**.



If you enter a wrong server address and re-enter the correct address, it could take the appliance a few minutes to find the NTP server.

It may take a few minutes to contact the server. If the system cannot contact the server, the request will time out in a few minutes and will take you to the next panel in the wizard. Make sure to resolve connectivity issues after completing the setup process.

The list of servers configured by default points ArcSight Express to a virtual cluster of time servers operated by the NTP project. Assuming that UDP port 123 is open to the

outside internet in your firewall, you can keep the default values, unless you would prefer to use your own cluster of NTP servers.



**Note**

Using NTP is strongly recommended, since accurate time keeping is essential for event correlation and log management. But if you choose to de-activate the Network Time Protocol, set the local date and time in the Date & Time tab.



**Note**

### Restarting this wizard if you exit it...

If you exit out of any of the screens from this point forward, the wizard will exit with the following warning:

The wizard is not finished yet. Are you sure you want to exit?

You can re-start the wizard at any point until you get to the screen which tells you that the appliance configuration is about to begin. To re-start the wizard, run the following command from

/opt/arcsight/manager/bin directory while logged in as user "root":

```
./arcsight appliancefirstbootsetup -boxster
```

The ArcSight Express appliance is functional only after successful completion of the wizard.

- 6 Select the language in which you want text to be displayed in the ArcSight Express user interface and click **Next**.
- 7 Set a password for your database (CORR-Engine) by entering it in the Database password textbox and reentering it in the Password confirmation textbox to confirm it. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration." Click **Next**:



- 8 Enter the maximum number of days you would like to retain the data and click **Next**.

- 9 Configure the following e-mail addresses:

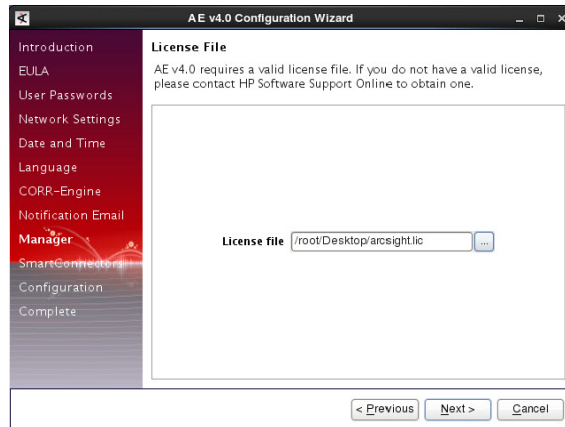
**Error Notification Recipients:** An e-mail address of the person who should receive e-mail notifications in the event that the ArcSight Manager goes down or encounters some other problem.

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

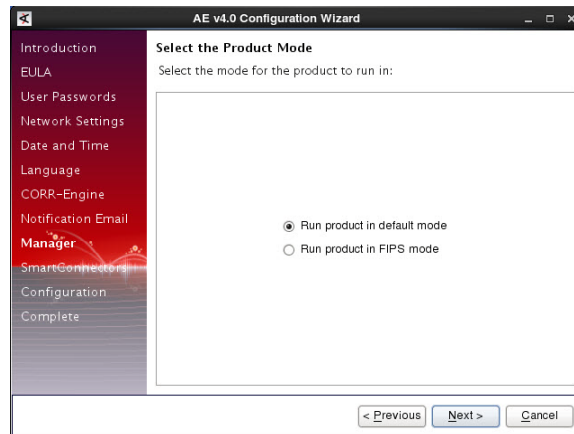
Click **Next**.

- 10 Enter or navigate to the location where you have placed the ArcSight Express appliance license zip file. You do not need to extract the license from the zip file. Click **Next**.

If you do not have a license file, contact HP ArcSight Customer Support to obtain one. You can use `scp` or `sftp` to get it onto the appliance.



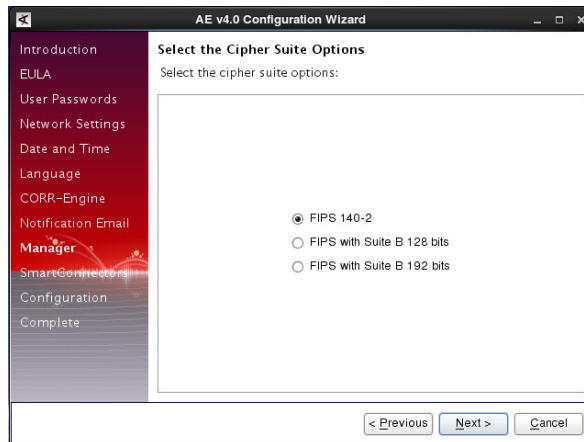
- 11** Select the mode in which you would like to configure the software components on ArcSight Express.



**Caution**

- Once you have configured ArcSight Express in FIPS mode, you will not be able to convert it to default mode without doing a factory reset.
- If you choose to configure ArcSight Express in FIPS mode, note that the container for the Syslog connector automatically gets FIPS-enabled. Since the Microsoft Windows Event Log -Unified connector does not support FIPS mode, its container will **not** be FIPS-enabled. If you would like to add additional containers, see the Connector Management User's Guide for details on how to do so. To install connectors in FIPS mode on a remote host (host other than ArcSight Express), see the individual connector's configuration guide. Once you have enabled FIPS on a remote host connector, you can manage it just like any other remote host connector using the Connector Management module. See the Connector Management User's Guide for details on managing remote host connectors.
- Converting an existing 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, section "Changing a Default Mode Installation to FIPS 140-2".
- By default, ArcSight Express 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 First Boot Wizard deployment completes successfully. Refer to the Administrator's Guide for details on using a CA-signed certificate.
- The self-signed certificate which is generated by default is valid for a limited period of time, after which you will have to regenerate it. For instructions on how to generate the self-signed certificate, refer to the Administrator's Guide.

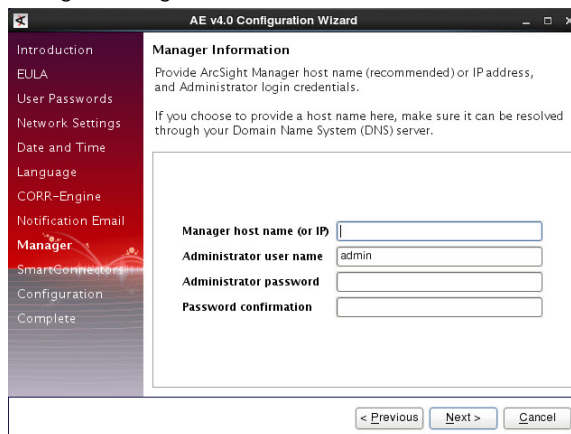
- 12 (If you selected FIPS mode only)** You will see a screen asking you to select the cipher suite.



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.

- 13** Enter the ArcSight Manager's host name or IP address, and configure information which will be used to create an ArcSight Manager user with administrative privileges. Click **Next**.

**Important:** Make sure to change the **Manager Host Name** to either the host name or IP address of the ArcSight Express appliance. The ArcSight Manager host name will be used to generate a self-signed certificate and also when accessing the ArcSight Manager using the ArcSight Console or the Management Console. The Common Name (CN) in the certificate will be the ArcSight Manager host name that you specify in the ArcSight Manager Information screen.



- 14** This screen will **not** appear if you are installing the product in Suite B mode. If you are setting up ArcSight Express in Suite B mode, and you would like to set up the Syslog Daemon and the Microsoft Windows Event Log - Unified connector, refer to their respective configuration guides for details on setting them up. If you are installing the

product in FIPS 140-2 mode, you will not see the option to set up the Microsoft Windows Event Log - Unified connector.

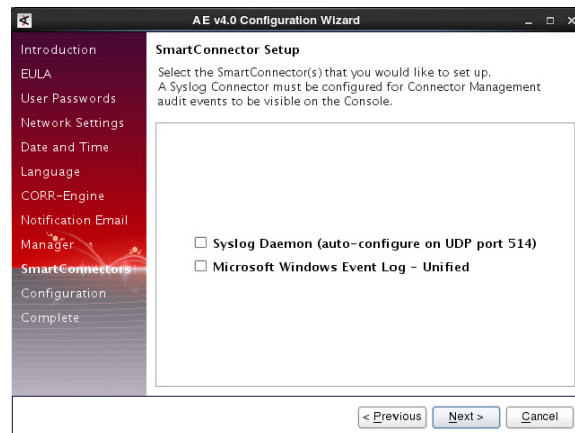


Do not set up the pre-bundled connectors in this screen if you plan to migrate your resources from Oracle to the CORR-Engine (from an older version of ArcSight Express appliance with Oracle). You can configure the connectors **after** you migrate the resources.

Select which pre-bundled SmartConnectors you want to install and configure. Setting up these SmartConnectors in this panel is optional. You can optionally set them up at any time later using the Connector Management tab on the Management Console. If you choose to configure the Microsoft Windows Event Log - Unified connector manually at a later time, you will need to configure the parser version to 1. Detailed Security Event mappings for this parser version can be found in Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1 (MSWindowsEventLogUnifiedMappingsParserVersion1.pdf), distributed with ArcSight Express 4.0 documentation.

For a complete list of connectors that you can install independently and use with ArcSight Express, refer to the article “Supported Products for Connector Appliance” from the ArcSight Knowledge Base.

The Syslog Daemon connector collects events from the logs that are sent by devices to the ArcSight Express appliance on port 514 using UDP. The Microsoft Windows Event Log - Unified connector collects events from the Windows hosts that you specify in the upcoming screens.



If you selected the Syslog Daemon connector, no further information is required. This First Boot Wizard automatically does the configuration for you. The connector is configured for UDP connection on port 514. If you want to use the TCP transport or another port for syslog event collection, you can modify the connector parameters using the Connector Management tab on the Management Console after completion of the installation. If you use any non default ports, make sure to open these ports on the appliance.

- 15 (For Microsoft Windows Event Log -Unified)** Enter the Active Directory domain information needed to identify the Windows Domain from which you will be collecting events. This wizard will automatically discover the Windows hosts that reside in this domain and present them in the next panel.



Make sure that the user that you specify in this screen has administrative privileges on the Domain and its hosts.

**AE v4.0 Configuration Wizard**

**Microsoft Windows Event Collection**  
Provide Microsoft Active Directory information to enable automatic discovery of your Windows hosts.

Domain Name:

Active Directory Server:

Domain Admin User Name:

Domain Admin Password:

< Previous Next > Cancel

Click **Next**.

- 16** Select the Windows operating system versions present on the hosts from which you would like events collected. You will be prompted to refine this selection in the next panel to remove individual hosts from the list if need be.

**AE v4.0 Configuration Wizard**

**Microsoft Windows Event Collection Log**  
Select the version(s) of the Windows operating system on the hosts from which you would like to collect Windows security events.

☒ Windows Server 2008 R2 (5 Hosts)

☒ Windows 7 (3 Hosts)

☒ Windows Vista (1 Hosts)

☐ Windows Server 2003 (6 Hosts)

☐ Windows XP (5 Hosts)

< Previous Next > Cancel

Click **Next**.

- 17** Select the specific hosts from which you want to collect the events. Events will be collected from the security event log and the system event log of the hosts selected in this panel.

**AE v4.0 Configuration Wizard**

**Microsoft Windows Event Collection Log**  
Select the Windows hosts from which to collect Windows security events.

<input checked="" type="checkbox"/>	Windows Version	Windows Host
<input checked="" type="checkbox"/>	Windows Server 2008 ...	N100-H010
<input checked="" type="checkbox"/>	Windows Server 2008 ...	N100-H045
<input checked="" type="checkbox"/>	Windows Server 2008 ...	N102-H088
<input checked="" type="checkbox"/>	Windows Server 2008 ...	N103-H191
<input checked="" type="checkbox"/>	Windows Server 2008 ...	WIN-S68G0M4OIH5
<input checked="" type="checkbox"/>	Windows 7	ADMIN-PC
<input checked="" type="checkbox"/>	Windows 7	N102-H032
<input checked="" type="checkbox"/>	Windows 7	N15-147-195
<input checked="" type="checkbox"/>	Windows Vista	N100-H192

< Previous Next > Cancel

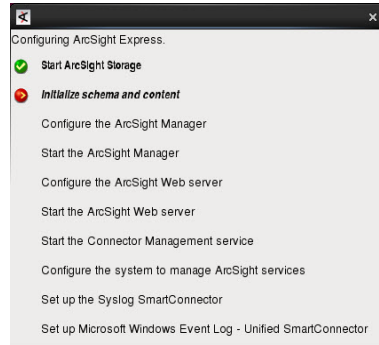
Click **Next**.

- 18 Review the summary of the hosts from which events will be collected and if satisfied, click **Next**.
- 19 You will see a screen that informs you that ArcSight Express is ready to be configured. If satisfied, click **Next** to continue with the configuration.



Keep in mind that once the wizard has started configuring the software components, if you exit the wizard or if an error occurs, you will have to configure that component manually.

- 20 You can see the progress and errors if any as the configuration process continues.



- 21 Once your appliance has been configured successfully, you will see a screen saying so. Click **Finish** in the Configuration Completed Successfully screen.

## Post Configuration Steps

- If you are using the Firefox web browser to access ArcSight Web, the Management Console, and the Connector Management in the Management Console, make sure to add an exception in the browser to allow it to import ArcSight Web's certificate and the Connector Management module's certificate. To do so:

**For ArcSight Web:**

- a Go to Firefox options (**Tools->Options**).
- b Click the **Advanced** tab.
- c Click the **Encryption** tab to bring it forward.
- d Click **View Certificates**.
- e Click **Add Exception**.
- f Enter the URL for the legacy web: `https://<manager URL>:9443`
- g Get the certificate and confirm the security exception.

**For Connector Management:**

- a Go to Firefox options (**Tools->Options**).
- b Click the **Advanced** tab.
- c Click the **Encryption** tab to bring it forward.
- d Click **View Certificates**.

- e Click **Add Exception**.
- f Enter the URL for the Connector Management module: `https://<manager URL>:6443`
- g Get the certificate and confirm the security exception.
- If your ArcSight Express appliance is configured in FIPS with Suite B mode, you will need to set up your connectors manually using the Connector Management module in the Management Console. Refer to the Connector Management User's Guide for details.
- If you did not set up the pre-bundled connectors (Syslog Daemon connector and the Microsoft Windows Event Log - Unified connector) while running the First Boot Wizard, you can add them later from the Connector Management module in the Management Console. When configuring the Microsoft Windows Event Log - Unified connector you will need to configure the parser version to 1. Detailed Security Event mappings for this parser version can be found in Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1 (MSWindowsEventLogUnifiedMappingsParserVersion1.pdf), distributed with ArcSight Express 4.0 documentation.
- You can set up the Forwarding Connector and the Reputation Security Monitor Model Import Connector after the First Boot Wizard completes.

The Reputation Security Monitor Model Import Connector is located in `/opt/arcsight/software/connector/repSmConnr/ArcSight-5.2.7.xxxx.0-RepSMMModelConnector-Linux64.bin`.

The Forwarding Connector is located in `/opt/arcsight/software/connector/forwardConnr/ArcSight-5.2.7.xx.xx.0-SuperConnector-Linux64.bin`. For details on how to install them, see the respective connector configuration guides for these connectors.
- The number of connectors, hosted on the ArcSight Express appliance, that the Connector Management module can manage depends on your license. The maximum is eight. ArcSight Express comes pre-bundled with two connectors, the Syslog Daemon connector and the Microsoft Windows Event Log - Unified connector. In addition to these two, you have the option to install up to six additional connectors on the appliance depending on your license. All connectors residing on the appliance must be managed by the Connector Management module. For a list of the additional connectors that can be installed on ArcSight Express, see the chapter, ["Using SmartConnectors" on page 55](#)
- You can install additional connectors (depending on your product license) on remote machines which can be remotely managed by ArcSight Express. For a list of the additional connectors that can be managed remotely, refer to the article Supported Products for Connector Appliance from the ArcSight Knowledge Base.
- For details on how to get the Connector Management module to manage them, see the Connector Management User's Guide.

The ArcSight Express appliance is ready for use.

## Setting Up SmartConnectors

Refer to the chapter, ["Using SmartConnectors" on page 55](#) for details on this.



## Setting Up Client-Side Authentication on SmartConnectors

To set up client-side authentication on SmartConnectors:

- 1 Follow the steps in the ESM Administrator's Guide in the section, "Setting up SmartConnectors with Client-side Authentication".
- 2 Once the client-side authentication has been enabled, go to the Connector Management tab in the Management Console and manually restart the container so that the changes take effect.

## To Set Up ArcSight Express 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 ArcSight Express.

### On the ArcSight Manager

This procedure is required only if you plan to output reports that use international characters in PDF format.

- 1 On the ArcSight Manager host, place the font file `ARIALUNI.TTF` in a folder. For example:

```
/usr/share/fonts/somefolder
```

- 2 Modify the reports properties file, `sree.properties`, located in `/opt/arcsight/manager/reports/` directory by default.

Add the following line:

```
font.truetype.path=/usr/share/fonts/somefolder
```

- 3 In the ArcSight Console UI, select the Arial Unicode MS font in all the report elements, including the report template.

### On the ArcSight Console

Set preferences in the ArcSight Console and on the host on which the ArcSight Console resides.

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

**On Windows:** Edit `console.bat`

**On Macintosh:** Edit `console.sh`

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

Find the section `ARCSIGHT_JVM_OPTIONS` and append the following jvm option:

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

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

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

**On Windows:** Select Arial Unicode MS from the drop-down

**On Linux:** Enter Arial Unicode MS

## The Next Steps

- Download the ArcSight Console and install it on a supported platform. The ArcSight Console should not be installed on the ArcSight Express appliance. Refer to the next chapter, [Installing ArcSight Console](#), for details on how to do this.
- If you have not already done so, read the Release Notes available on the HP ArcSight Customer Support download site.

# Running the ArcSight Manager Configuration Wizard

---

This chapter covers the following topics:

[“Running the Wizard” on page 27](#)

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

## Running the Wizard

We recommend running the wizard as user “arcsight”. Before you run the `managersetup` wizard, stop your ArcSight Manager by running the following command:

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

Verify that the ArcSight Manager has stopped by running the following command:

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

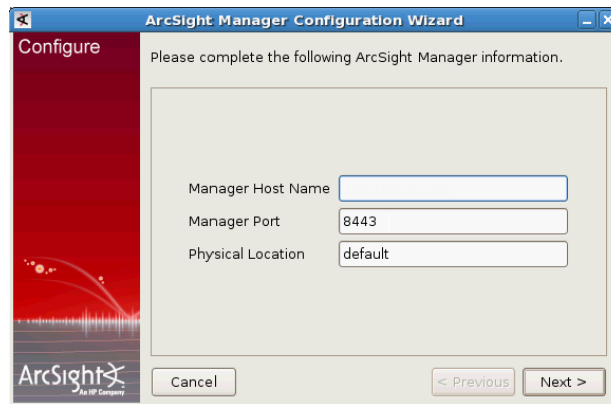
To start the `managersetup` wizard, run the following from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

The `managersetup` wizard will start.

- 1 Select the mode in which to run the ArcSight Manager, default or FIPS mode.
- 2 If you would like to change the hostname or IP address for your ArcSight Express appliance, enter the host name or IP address of your ArcSight Express machine. Keep in mind that the ArcSight Manager host name that you enter in this dialog will appear on the ArcSight Manager certificate. If you do change the ArcSight Manager host

name, be sure to regenerate the ArcSight Manager's certificate in [Step 5 on page 29](#). We recommend that you do not change the ArcSight Manager Port number.



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

The managersetup Configuration Wizard establishes parameters required for the ArcSight Manager to start up when you boot up the ArcSight Express appliance.

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



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard, specifically the license selection screen. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area contains the text: 'You presently have a license file installed. License String: Internal license, used for development and QA. Customer: ArcSight Internal License Key, Expiration date: 2011/06/30. Would you like to keep it or replace it with another license file?'. Below this are two radio buttons: 'Keep the current license file.' (selected) and 'Replace current license file.'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

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

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



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard, specifically the Java Heap Memory Size screen. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area contains the text: 'The heap size is the amount of memory that ArcSight Manager will use. Please set the following memory parameter as appropriate for this host.' Below this is a dropdown menu labeled 'Java Heap Memory Size (MB)' with '8192' selected. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

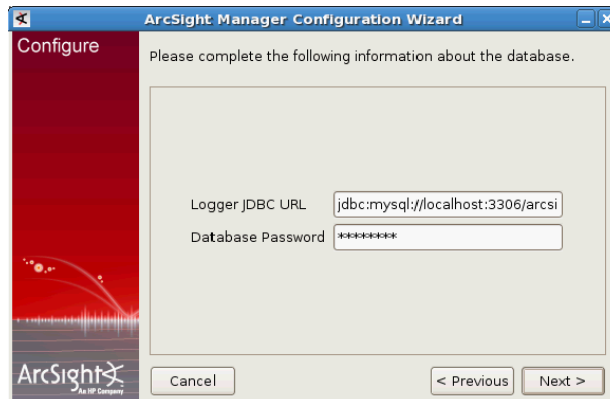
The Java Heap memory size is the amount of memory that ArcSight Express will allocate for its heap. (Besides the heap memory, the ArcSight Manager on the ArcSight Express uses some additional system memory as well.)

- 5 The ArcSight Manager controls SSL certificate type for communications with the ArcSight Console, so the wizard prompts you to select the type of SSL certificate that the ArcSight Manager is using. If you had changed the ArcSight Manager host name in [Step 2 on page 27](#), select **Replace with new Self-Signed key pair**, otherwise select **Do not change anything**.



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

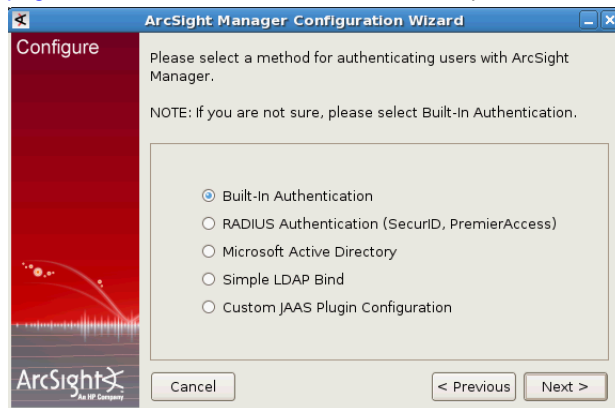
- 6 Accept the default in this screen and click **Next**.



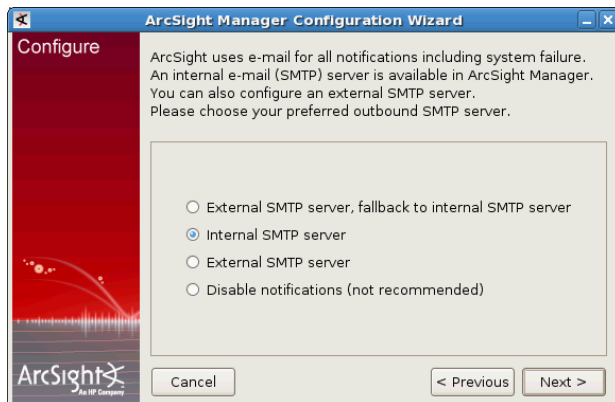
- 7 Select the desired authentication method and click **Next**.



- 8 Select the method for authenticating the users. See [“Authentication Details” on page 32](#) for more details on each of these options.



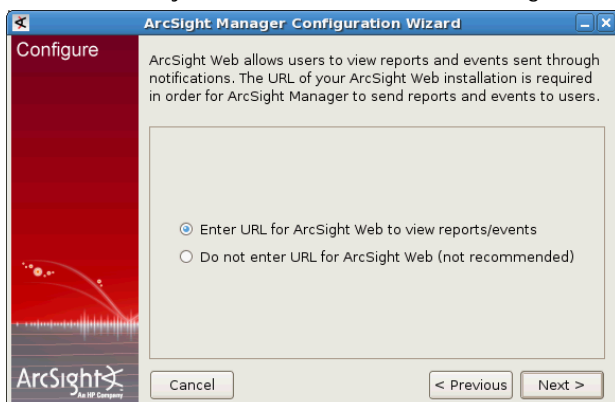
- 9 Accept the default and click **Next** or configure a different email server for notification.



**Caution**

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

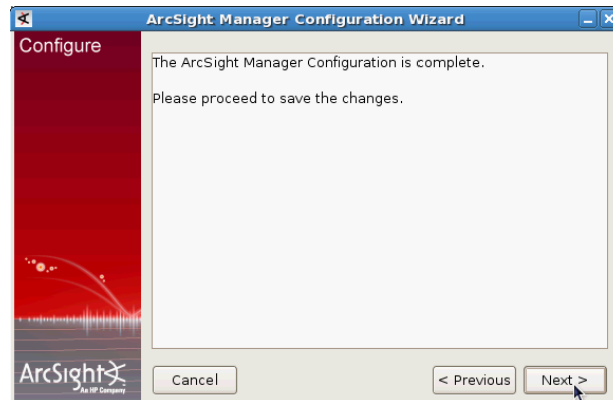
- 10 Enter one or more email address(es) (separated by commas) where you want the failure notifications to go.
- 11 Select whether you want to get email notifications in the event of failures or opt to disable the email notifications.
- 12 Select whether you want to enter a URL for ArcSight Web and click **Next**.



- 13** If you opted enter a URL for ArcSight Web, you will see a screen in which you must enter the URL for ArcSight Web server.
- 14** ArcSight Manager can automatically create an asset when it receives an event with a new sensor or device information. By default, assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation**.



- 15** Click **Next** in the following screen.



- 16** Click **Finish** in the following screen:



You have completed the ArcSight Manager setup program. You can now start the ArcSight Manager by running the following:

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

## Authentication Details

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



**Caution**

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

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

---

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

### How external authentication works

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

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

Users who pass these checks are authenticated.

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

### Guidelines for setting up external authentication

Follow these guidelines when setting up an external authentication mechanism:

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



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



**Caution**

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

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

## Password Based Authentication

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

### Built-In Authentication

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

If you selected this option, you are done.

### Setting up RADIUS Authentication

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

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

## Setting up Active Directory User Authentication

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

The next panel prompts you for this information.

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

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

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

### Configuring AD SSL

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

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

## Setting up LDAP Authentication

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

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

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

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



**Note**

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

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

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

## Configuring LDAP SSL

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

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

## Using a Custom Authentication Scheme

From the Manager Setup Wizard, you can choose the **Custom JAAS Plug-in Configuration** option if you want to use an authentication scheme that you have built. (Custom Authentication is not supported from the ArcSight Management Console.) You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.

## Password Based and SSL Client Based Authentication

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



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

---

## Password Based or SSL Client Based Authentication

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

## SSL Client Only Authentication

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

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

## Chapter 4

# Installing ArcSight Console

---

The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of ArcSight Web or the Management Console) to ArcSight Express. This chapter explains how to install and configure the ArcSight Console in default mode. To install the ArcSight Console in FIPS mode, see [Appendix E, ArcSight Express in FIPS Mode, on page 103](#). Section [“Choosing between FIPS Mode or Default Mode” on page 11](#) lists the basic differences between the three modes.

The following topics are covered in this chapter:

[“ArcSight Console Supported Platforms” on page 37](#)

[“Using a PKCS#11 Token” on page 38](#)

[“Installing the ArcSight Console” on page 39](#)

[“Starting the ArcSight Console” on page 50](#)

[“Reconnecting to the ArcSight Manager” on page 52](#)

[“Reconfiguring the ArcSight Console” on page 53](#)

[“Uninstalling the ArcSight Console” on page 53](#)

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

## ArcSight Console Supported Platforms

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

## Required Libraries on the RHEL 6.2 64 Bit Workstation

On the RHEL 6.2 64-bit Workstation, the ArcSight 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 Express 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 D, Using the PKCS#11 Token, on page 91](#) for details on using a PKCS #11 token with the ArcSight Console.

## Installing the ArcSight 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 ArcSight Console. Refer to the Release Notes for the version of JRE to install
- If you are installing the ArcSight Console on a new system for the first time, or if you have upgraded your system causing the JRE update, your ArcSight 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 ArcSight 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 ArcSight Console, change the default password for the cacerts file in the `/current/config/client.properties` file (create the file if it does not exist) by adding: `ssl.truststore.password=changeme`

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

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

Platform	Installation File
Linux	<code>ArcSight-6.1.0.xxxx.y-Console-Linux.bin</code>
Windows	<code>ArcSight-6.1.0.xxxx.y-Console-Win.exe</code>
Macintosh	<code>ArcSight-6.1.0.xxxx.y-Console-MacOSX.zip</code>

- 1 Click **Next** in the Installation Process Check screen.
- 2 Read the introductory text in the Introduction panel and click **Next**.
- 3 The "I accept the terms of the License Agreement" radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read the text click the "I accept the terms of the License Agreement" radio button and click **Next**.
- 4 Read the text in the Special Notice panel and click **Next**.

- 5 Navigate to an existing folder where you want to install the ArcSight Console or accept the default and click **Next**. If you specify a folder that does not exist, the folder gets created for you.



- On Linux and Macintosh systems, spaces are not supported in install paths.
- **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 ArcSight 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 ArcSight 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 ArcSight 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 in the Installing ArcSight Express Console 4.0 screen.

## Character Set Encoding

Install the ArcSight Console on a machine that uses the same character set encoding as the ArcSight 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 ArcSight 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 ArcSight 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 ArcSight Console where these users would log in. In that situation, add the following property to the

console.properties file:

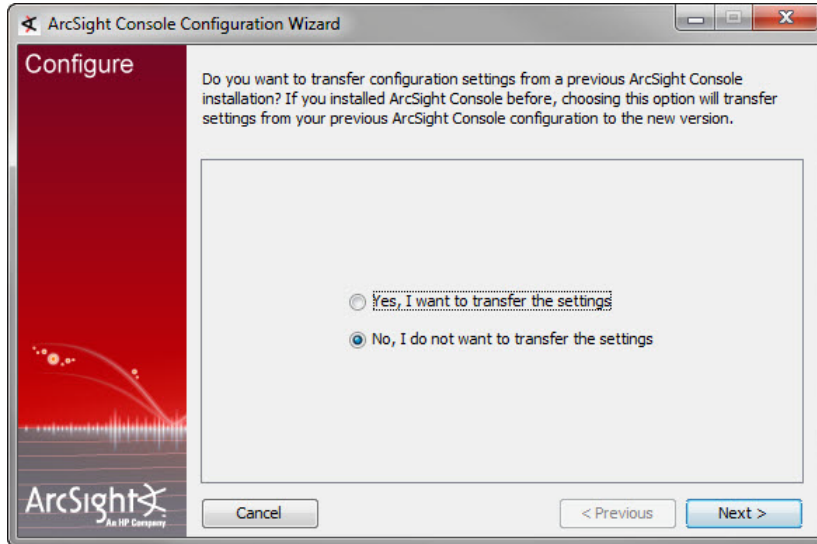
console.ui.enable.shortcut.schema.persist=false. This property prevents custom shortcut key schema changes or additions.

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



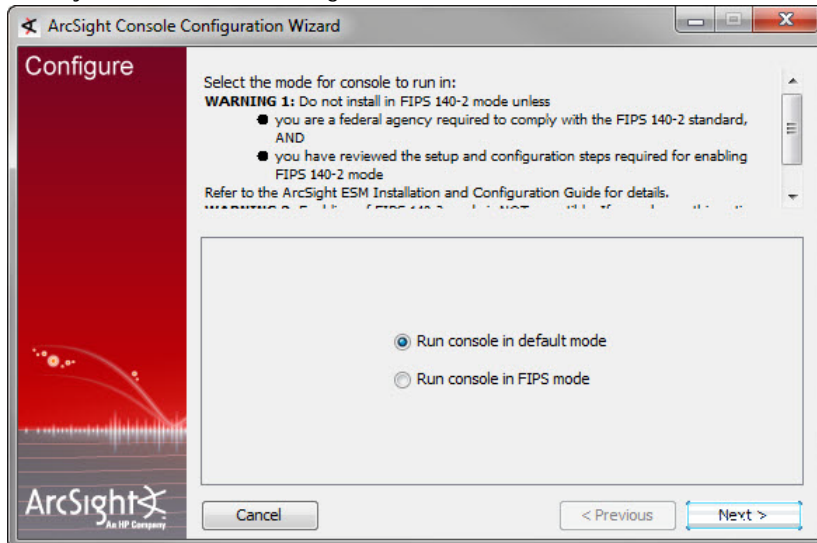
## Configuration Settings

After the ArcSight 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**.



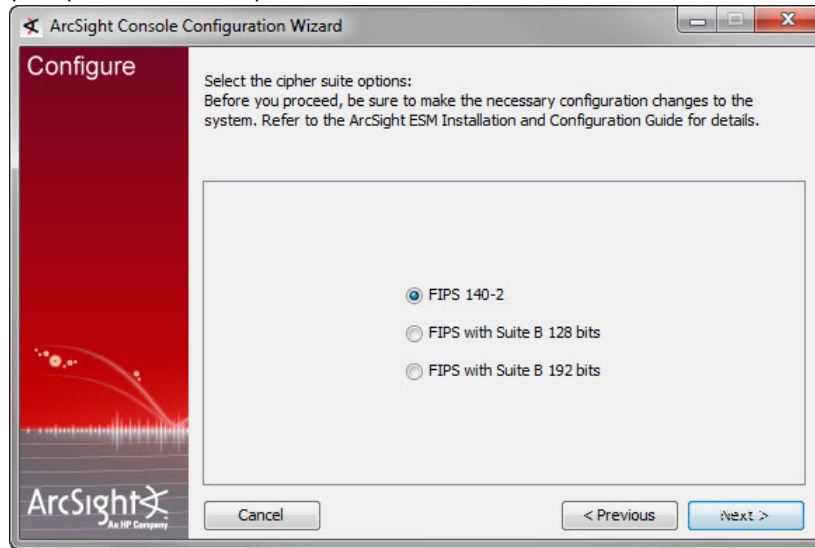
## Selecting the Mode in which to Configure ArcSight Console

Next, you will see the following screen:



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

If you selected **Run console in FIPS mode**, you will be informed that you cannot revert to default mode once you proceed with FIPS mode. If you click on **Yes**, 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**.

## ArcSight Manager Connection

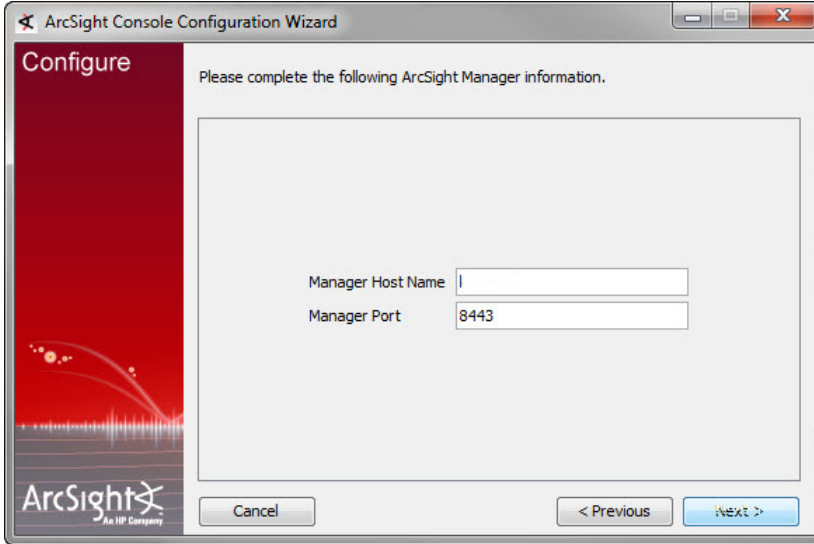
The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. Enter the host name or IP address of the ArcSight Manager to which the ArcSight Console will connect.



**Caution**

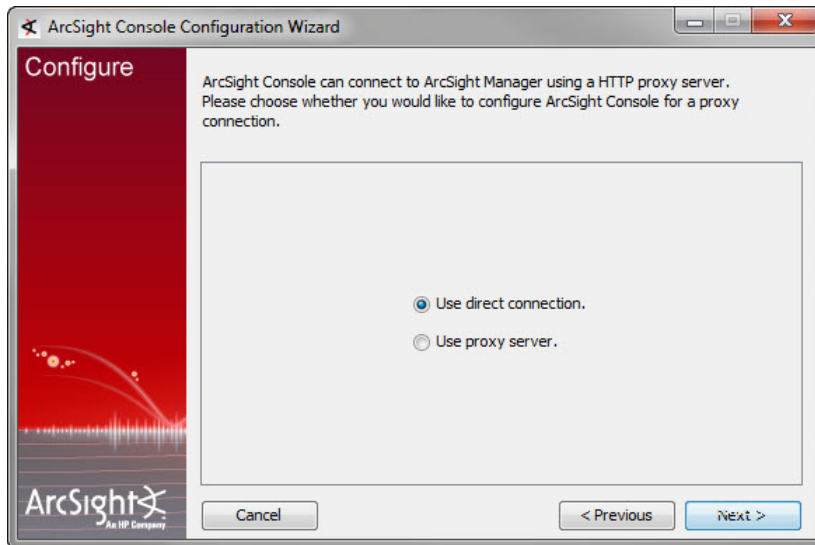
Do not change the ArcSight Manager's port number.

Click **Next**.



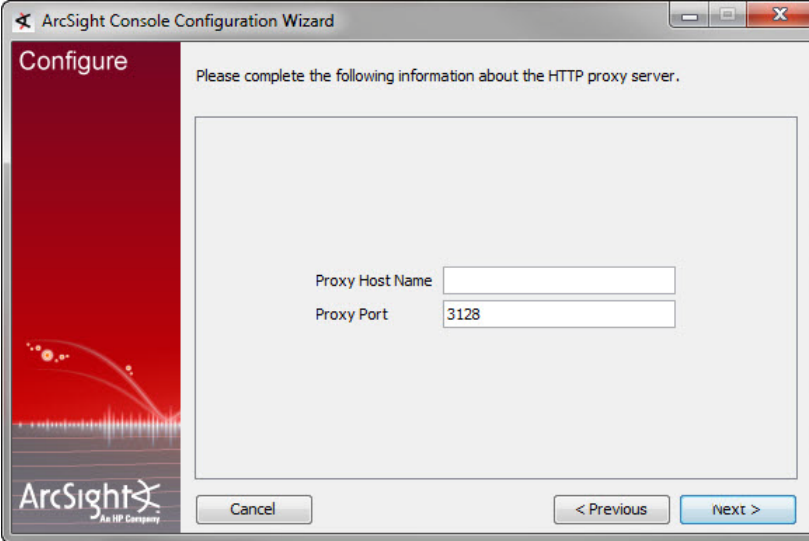
The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. On the left is a red sidebar with the ArcSight logo and the text 'An HP Company'. The main area has a light gray background with the text 'Please complete 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 >'.

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



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 the text 'An HP Company'. 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 >'.

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. The title bar reads 'ArcSight Console Configuration Wizard'. The window has a red sidebar on the left with the word 'Configure' at the top and the ArcSight logo at the bottom. The main area is light gray and 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 are three buttons: 'Cancel', '< Previous', and 'Next >'. The 'Next >' button is highlighted in blue.

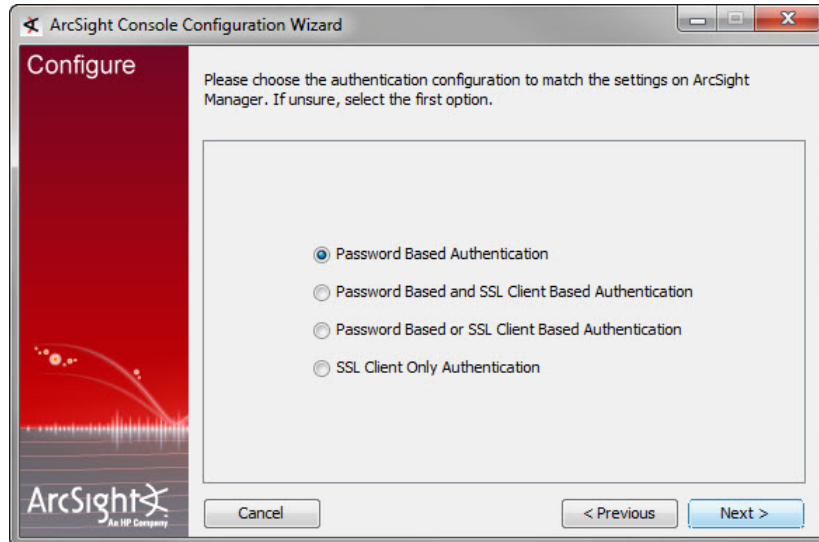
Enter the Proxy Host name and click **Next**.

## Authentication



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

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

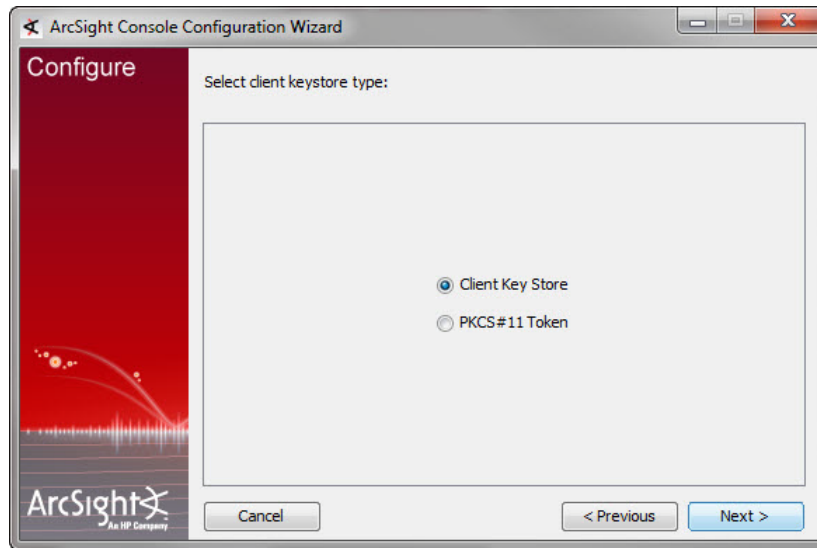


**Password Based and SSL Client Based Authentication** option currently supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method within the **Password Based and SSL Client Based Authentication** option is not currently supported.

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

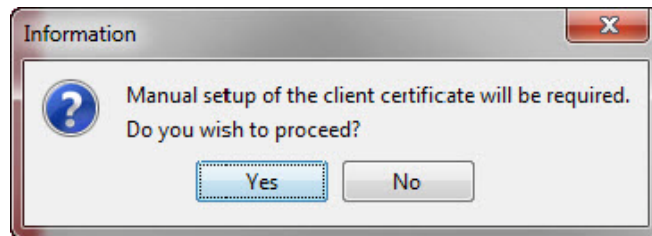
If you select **Password Based and SSL Client Based Authentication**, you will be required to enter both user name/password combination and you will be required to setup your client certificate manually. Follow the procedure described in the ArcSight Express Administrator's Guide to set up the client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



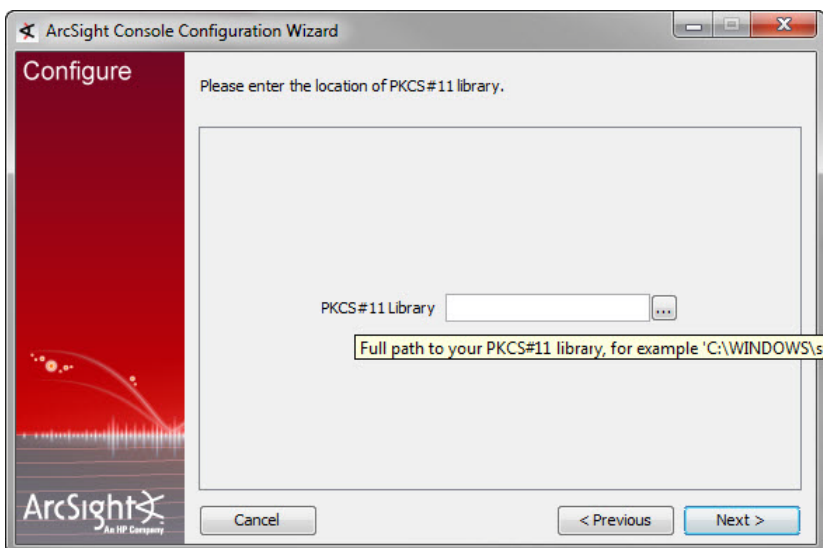
If you plan to use a PKCS #11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the ArcSight Console, you can refer to [Appendix D, Using the PKCS#11 Token, on page 91](#) 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 ArcSight Express Administrator's Guide to set up the client certificate.

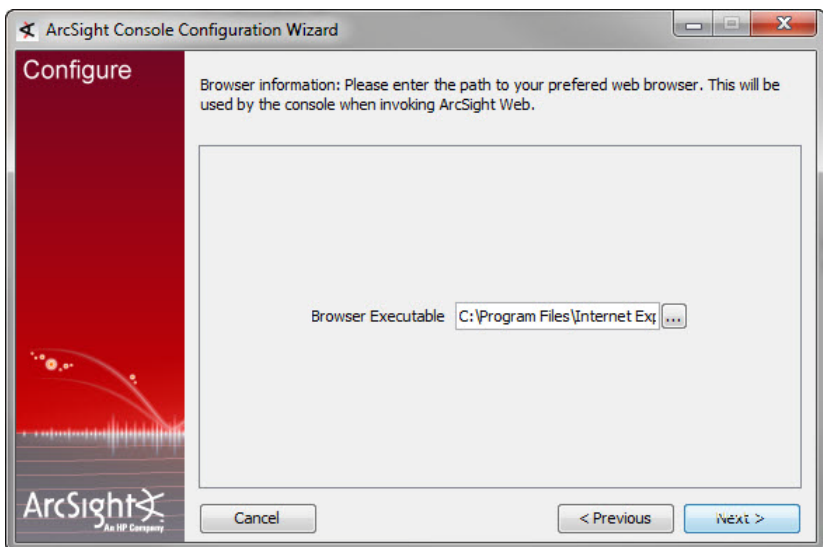
If you selected PKCS #11 Token, you will be prompted to enter the PKCS #11 library location.

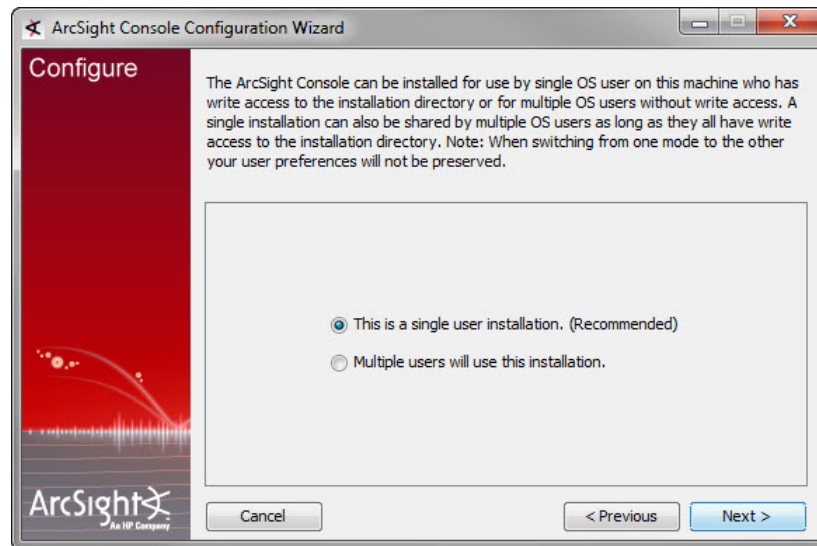


## Web Browser

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 ArcSight Console users will use to connect to the ArcSight Console. For example, a system account, admin, is used by ArcSight Console users Joe, Jack, Jill, and Jane.

OR

- ◆ All ArcSight Console users who will use this machine to connect to the ArcSight 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 ArcSight 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 ArcSight Console users are located centrally in ArcSight Console's `\current`.

**Disadvantage:** You cannot use this option if your security policy does not allow all ArcSight 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 ArcSight Console users who will be using this machine to connect to the ArcSight 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 ArcSight Console users to the ArcSight 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 ArcSight Console users to the ArcSight Console's `\current` directory, they can only run the following commands (found in the ArcSight Console's `bin\scripts`) from the ArcSight Console command-line interface:

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

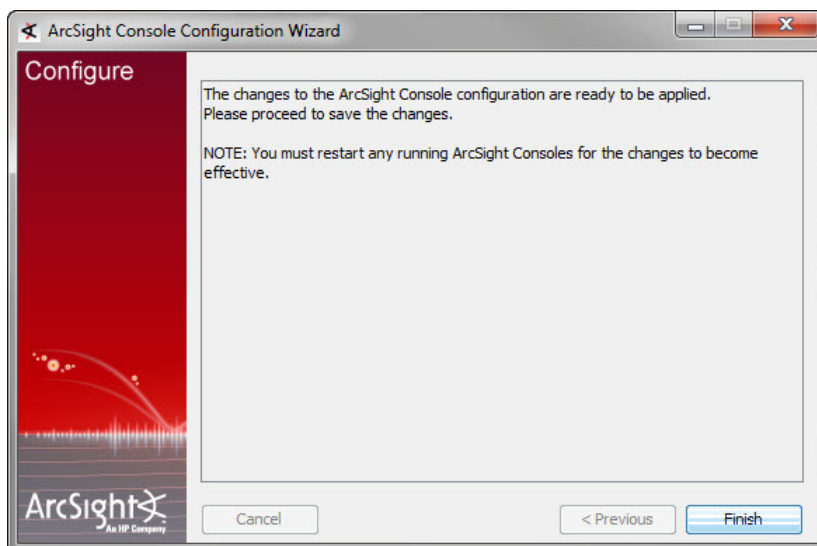
All other commands require write permission to the ArcSight Console's `\current` directory.



Note

The location from which the ArcSight 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 ArcSight Console is currently configured with the "This is a single system user installation" option on a Windows machine. ArcSight Console user Joe's customized preferences file is located in the ArcSight 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 ArcSight Console, the ArcSight 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 last screen.



---

**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 ArcSight Console, you need to change the default password for the cacerts file in the ArcSight Console's `\current\config\client.properties` file (create the file if it does not exist). Add the following line:

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

---

## Importing the ArcSight Console's Certificate into the Browser

The online help from the ArcSight 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 ArcSight Console. You will need to do this using the `keytoolgui`. Refer to the Administrator's Guide for ArcSight Express in the "Using Keytoolgui to Export a Key Pair" section.
- 2 Import the ArcSight Console's keypair into the Browser. Refer to the Administrator's Guide for details on how to do this.

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

## Starting the ArcSight Console

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

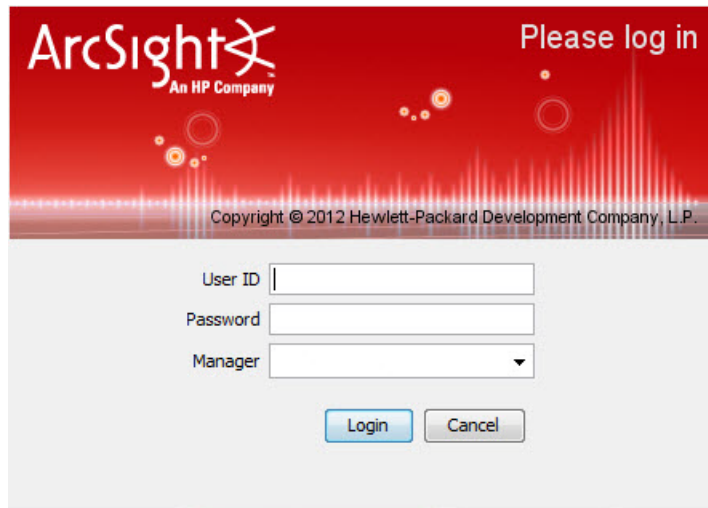
To start the ArcSight Console, use the shortcuts installed or open a command window from the ArcSight Console's `bin` directory and run:

On Windows:

```
arcsight console
```

On Unix:

```
./arcsight console
```



The image shows the ArcSight login interface. At the top, there is a red banner with the ArcSight logo (An HP Company) on the left and the text 'Please log in' on the right. Below the banner, the copyright notice 'Copyright © 2012 Hewlett-Packard Development Company, L.P.' is visible. The main login area has a light gray background and contains three input fields: 'User ID', 'Password', and 'Manager' (a dropdown menu). Below these fields are two buttons: 'Login' (highlighted in blue) and 'Cancel' (gray).

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

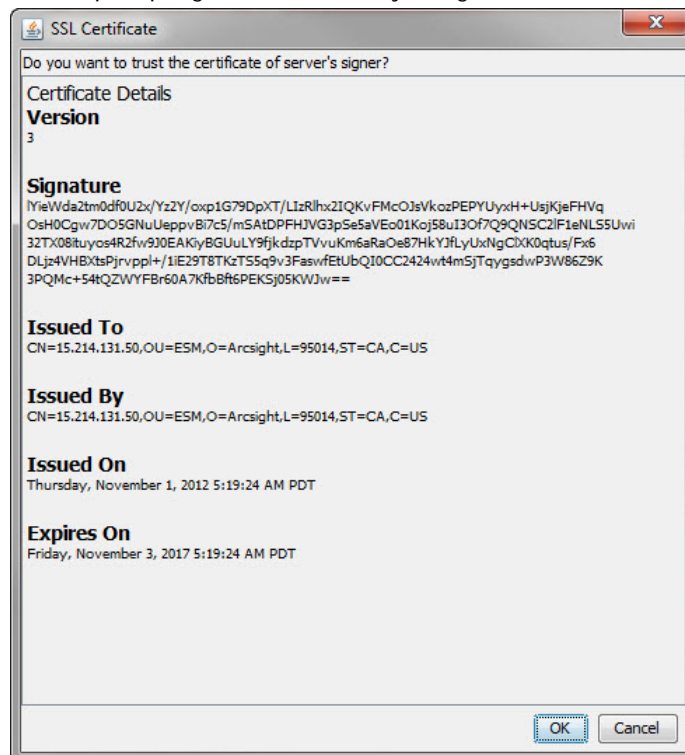
If you selected...	You will see the following buttons...
Password Based Authentication	Login Cancel
Password Based and SSL Client Based Authentication	Login Cancel
Password Based or SSL Client Based Authentication	If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: 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 ArcSight Console



While logging into an ArcSight 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 ArcSight Console.

To start the ArcSight Console, click **Login**. When you start the ArcSight Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the ArcSight Manager's certificate. The prompt will show details specific to your settings (following is just an example). Click **OK** to trust the ArcSight Manager's certificate. The certificate will be permanently stored in the ArcSight 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 ArcSight 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 ArcSight 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 ArcSight 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 Express Console ->Uninstall ArcSight Express Console 4.0**

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

`Uninstall_ArcSight_Express_Console.exe`

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

`./Uninstall_ArcSight_Express_Console`



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



## Chapter 5

# Using SmartConnectors

---

This chapter covers the following topics:

[“Installing SmartConnectors” on page 55](#)

[“ArcSight SmartConnectors with ArcSight Express” on page 56](#)

[“Importing the Manager’s Certificate” on page 62](#)

ArcSight SmartConnectors provide easy, scalable, audit-quality collection of all logs from all event-generating sources across the enterprise for realtime and forensic analysis. SmartConnectors process raw data generated by various security vendor devices throughout an enterprise. Devices are hardware and software products such as routers, anti-virus products, firewalls, intrusion detection systems (IDS), VPN systems, anti-DoS appliances, operating system logs, and other sources that detect and report security or audit information.

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

## Installing SmartConnectors

The connectors that reside on the ArcSight Express appliance are managed by the Connector Management module. You can manage connectors remotely, too.

Installing and configuring the SmartConnector on the ArcSight Express system is a three step process:

- 1** Install the SmartConnector.

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

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

- 3** Configure the SmartConnector.

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

## ArcSight SmartConnectors with ArcSight Express

Included (pre-bundled) with ArcSight Express are two SmartConnectors, the SmartConnector for Syslog Daemon and the SmartConnector for Microsoft Windows Event Log - Unified, which collect events from system logs (syslog) and from Microsoft Windows Event Logs.

After initial installation with the First Boot Wizard, you can add connectors, depending upon your individual license agreement. The connectors available with ArcSight Express are:

- Blue Coat Proxy SG Multiple Server File
- Cisco Secure IPS SDEE
- IBM SiteProtector DB
- McAfee ePolicy Orchestrator DB
- McAfee Vulnerability Manager DB
- McAfee Network Security Manager DB
- Microsoft SQL Server Audit Multiple Instance DB
- Microsoft Windows Event Log - Unified
- Oracle Audit DB
- Sourcefire Defense Center eStreamer
- Symantec Endpoint Protection DB
- Trend Micro Control Manager DB
- Snort DB
- Syslog Daemon

The ESM Forwarding Connector and the SmartConnector for Reputation Security Monitor (RepSM) used in conjunction with the Reputation Security Monitor Solution are both available with ArcSight Express as well (but are installed after the First Boot Wizard completes).

For the current list of SmartConnector supported for management on Connector Appliance, including those that require additional setup, refer to the article [Supported SmartConnectors for Connector Appliance](#) from the ArcSight Knowledge Base. Search for the Knowledge Base article under the **Self-solve** tab on the HP SSO site.

## First Boot Wizard Configuration

During initial configuration, SmartConnector Setup lets you select Syslog Daemon and Microsoft Windows Event Log - Unified connectors.

If you select Syslog Daemon, no further information is required. The connector is configured for UDP connection on port 514. If you want to use the TCP transport or another port for syslog event collection, you can modify the connector parameters after installation is complete. See [“Update Connector Parameters” on page 62](#) for details.

If you select Microsoft Windows Event Log - Unified, the next window prompts you for information needed to identify the Windows Domain from which you will be collecting events. You can then select from which Windows hosts events are to be collected, and are given an opportunity to refine your selections. After you have provided this information, set up is complete, and configuration of ArcSight Express begins when you click **Continue**.



You can modify the parameters for this connector after the completion of the First Boot Wizard installation.

## About Pre-Bundled Connectors

These two connectors are included with ArcSight Express.

### The Microsoft Windows Event Log - Unified SmartConnector

System administrators use the Windows Event Log for troubleshooting errors. Each entry in the event log can have a severity of Error, Warning, Information, plus Success Audit or Failure Audit.

The SmartConnector for Microsoft Windows Event Log - Unified can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs and is optimized for a large number of hosts. This connector supports event collection from Microsoft Windows Server 2000, XP, Server 2003, Vista, Server 2008, Server 2008 R2, and Windows 7, as well as support for partial event parsing based upon the Windows event header for all System and Application events.

Some individual Windows Event Log applications are supported by the SmartConnector for Microsoft Windows Event Log - Unified, for which Windows Event Log sub-connectors have been developed. These sub-connectors have individual configuration guides that provide setup information and mappings for the particular application. These sub-connectors include:

- Microsoft Windows Event Log -- Unified: Microsoft Active Directory
- Microsoft Windows Event Log -- Unified: Microsoft Exchange Access Auditing for Exchange 2007 R2
- Microsoft Windows Event Log - Unified: Microsoft Forefront Protection 2010
- Microsoft Windows Event Log - Unified: Microsoft Network Policy Server
- Microsoft Windows Event Log - Unified: Microsoft Remote Access
- Microsoft Windows Event Log -- Unified: Microsoft SQL Server Audit
- Microsoft Windows Event Log -- Unified: Oracle Audit
- Microsoft Windows Event Log - Unified: NetApp Filer
- Microsoft Windows Event Log - Unified: Symantec Mail Security

The SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified provides information for enabling application support. Supplemental configuration guides provide specific mappings and setup information for each application.



**Note**

Security events are not audited by default. Be sure to specify the type of security events to be audited.

---

### The Syslog Daemon SmartConnector

Syslog messages are free-form log messages prefixed with a syslog header consisting of a numerical code (facility + severity), timestamp, and host name. These connectors can be installed as a syslog daemon (which is pre-installed), pipe, or file connector. Unlike other file connectors, a syslog connector can receive and process events from multiple devices. There is a unique regular expression that identifies the device. Syslog Daemon connectors

listen for syslog messages on a configurable port, using port 514 as a default. The default protocol is UDP, but other protocols such as Raw TCP are also supported. It is the only syslog option supported for Windows platforms.

The SmartConnector for UNIX OS Syslog provides the base parser for all syslog sub-connectors. For syslog connector deployment information, see the SmartConnector Configuration Guide for UNIX OS Syslog. For device-specific configuration information and field mappings, see the SmartConnector Configuration Guide for the specific device. Each syslog sub-connector has its own configuration guide.

The Syslog SmartConnectors use a sub-connector architecture that lets them receive events from different types of devices all sending syslog events. For example, the same SmartConnector can process events from a Cisco Router and a Juniper JUNOS device simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

ArcSight Express-supported Syslog sub-connectors include the following devices. For complete device configuration, parameter, and field mapping information for these connectors, see the appropriate SmartConnector Configuration Guide.

- Cisco PIX/ASA Syslog
- Cisco IOS Router Syslog
- Juniper Network and Security Manager Syslog
- Juniper JUNOS Syslog
- UNIX OS Syslog

## Set Up Pre-Bundled Connector Devices

During initial installation with the First Boot Wizard, you can select Syslog Daemon and Microsoft Windows Event Log - Unified connectors. There are some tasks to be performed to ensure Windows Event Log and Syslog devices have been set up to send events to the SmartConnectors.

### Syslog

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually. See [“Update Connector Parameters” on page 62](#) for more information.

If selected for install in the First Boot Wizard, the SmartConnector for Syslog Daemon is configured for you with ArcSight Express no further configuration is needed. See your device product documentation for information about setting up the device to send syslog events. This information also is provided in the SmartConnector Configuration Guide for the specific device, as well as specific event mappings to ArcSight fields.

## Microsoft Windows Event Log - Unified

If you selected and configured this connector during initial configuration, it has already been configured. Event collection is enabled for security and system events only.



When ArcSight Express is installed in FIPS mode, the container for the onboard Windows Event Log - Unified connector must not be FIPS-enabled in order for the connector to collect events.

Support is provided for a FlexConnector-like framework that lets you create and deploy your own parsers for parsing the event description for all system and application events. See "Create and Deploy Parsers for System and Application Events" in the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for more information.

Complete setup, installation, and configuration information about this connector is provided in the configuration guide for the SmartConnector for Microsoft Windows Event Log - Unified.

The on-board Windows Event Log Unified connector requires little configuration information; most of the configuration is done for you. When you install additional Windows Event Log Unified connectors, you will be required to provide more information, and the configuration guide will guide you through the process. For step by step instructions, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified.

Some individual Windows Event Log applications are supported by the SmartConnector for Microsoft Windows Event Log - Unified, for which Windows Event Log sub-connectors have been developed. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Protect 724:

- Microsoft Active Directory Windows Event Log Unified
- Microsoft Exchange Audit Windows Event Log - Unified
- Microsoft Forefront Protection 2010 for Exchange Windows Event Log - Unified
- Microsoft Network Policy Server Windows Event Log - Unified
- Microsoft Remote Access Windows Event Log - Unified
- Microsoft SQL Server Audit Windows Event Log - Unified
- NetApp Filer Event Log
- Oracle Audit Windows Event Log - Unified
- Symantec Mail Security Windows Event Log

Security events are not audited by default. You must:

- Enable Microsoft Windows Event Log Audit Policies
- Set Up Standard User Accounts on Your Domain Controller

Because event information generated by Windows servers is based upon which auditing policies are enabled, you should ensure the appropriate auditing policies are enabled on those Windows servers from which ArcSight will be collecting information. By default, none of the Windows auditing features are turned on.

When planning which events to audit, keep in mind that auditing events consumes system resources such as memory, processing power, and disk space. The more events you audit,

the more of these resources are consumed. Auditing an excessive number of events may dramatically slow down your servers.

You must be logged on as an administrator or a member of the **Administrators** group to set up audit policies. If your computer is connected to a network, network policy settings might also prevent you from setting up audit policies.

The method used to create an audit policy varies slightly depending upon whether the policy is being created on a member server, a domain controller, or a stand-alone server.

- To configure a domain controller, member server, or workstation, use **Active Directory Users and Computers**.
- To configure a system that does not participate in a domain, use **Local Security Settings**.

For step by step instructions, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified.

## General Information

### Authentication

To enable SSL authentication for connectors, follow the steps in "Setting Up SmartConnectors with Client Side Authentication" in the ArcSight Express Administrator's Guide. After client side authentication has been set up, manually restart the container on the appliance to implement the changes.

### ArcSight Services

Connectors on ArcSight Express are automatically installed as a service.

### FIPS Support

On the ArcSight Express appliance, FIPS support is enabled not by individual connector, but by container. For details on enabling or disabling FIPS mode on a container, see "Viewing Certificates on a Container" in the Connector Management for ArcSight Express 4.0 User's Guide.

### FIPS Compliant Connectors

- All syslog connectors
- All file reader connectors
- All SNMP connectors
- All database connectors (except when using Oracle drivers or SQL Server drivers with encryption)
- Cisco Secure IDS RDEP (Legacy) and Cisco Secure IPS SDEE connectors
- Sourcefire Defense Center eStreamer connector

### Non-FIPS Compliant Connectors

- Microsoft Windows Event Log - Unified
- Database connectors using SQL Server drivers with encryption
- Connectors using Oracle drivers
- Connectors running on AIX or HP UX platforms only

## Caveats

**FIPS Suite B Mode:** ArcSight Express does not support FIPS Suite B option for First Boot Wizard connector setup. After the boot process is complete, configure Suite B support for the connectors using the destination update options available in the connector configuration wizard.

**FIPS 140-2:** When ArcSight Express is installed in FIPS mode, the container for the onboard Windows Event Log - Unified connector must not be FIPS-enabled in order for the connector to collect events.

**Microsoft SQL 2005 JDBC Driver:** If you are running a database connector that uses the SQL 2005 JDBC driver with encryption enabled, the connector cannot be installed in FIPS-compliant mode. With encryption turned off, the MS SQL Server 2005 JDBC driver version 1.1 rather than 1.2 of the SQL Server 2005 JDBC driver should be used.

## Connector Upgrade

After ArcSight Express upgrade, no connectors are pre-installed or configured. There are no on-board connectors after upgrade, and all connectors must be installed after upgrade. See the SmartConnector Configuration guide for individual connectors for installation steps.

## Add Connectors

In ArcSight Express, you add connectors using the Connector Management module. Depending upon your license agreement, you can add connectors to ArcSight Express. Each connector should be added in its own container.

The configuration guide for each SmartConnector provides specific setup and configuration information for the individual connector, and provides mappings from vendor to ArcSight fields. Note that, when you add a connector on ArcSight Express, it is automatically configured as a service.

To add a connector, make sure the container, host, and location to which you want to add the connector exist on the system. Each connector on ArcSight Express should be installed in a separate container.

With the container selected, click the appropriate icon to add a connector. Select the connector you want to install from the drop-down list, enter the parameter values for the connector you selected, and follow the wizard through the configuration process.

For complete details, see "Adding a Connector" in the Connector Management for ArcSight Express 4.0 User's Guide.

## Model Import Connector for RepSM

ArcSight Express provides a free trial version of the Reputation Security Monitor (RepSM) Solution.

The Reputation Security Monitor (RepSM) solution uses internet reputation data to detect Advance Persistent Threats and zero day attacks as well as provide context to security events. The Model Import Connector for RepSM retrieves reputation data from the RepSM threat intelligence service (powered by HP DV Labs), processes this data, and forwards it to ArcSight ESM.

The HP Reputation Security Monitor Solution Guide describes how RepSM works and what it can do for you, and provides complete information for installing and configuring RepSM. This includes installing RepSM content, configuring Active Lists, and categorizing assets.

You can set up the Monitor Model Import Connector for RepSM after the First Boot Wizard completes. The Reputation Security Monitor Model Import Connector is located in `/opt/arcSight/software/connector/repSmConnr/ArcSight-5.2.7.xxxx.0-RepSMModelConnector-Linux64.bin`. The Configuration Guide for the Model Import Connector for RepSM describes the product and how to install the connector, as well as describing administrative tasks, such as setting up the Model Import user in ESM, starting and stopping imports, and reloading RepSM data.

## ESM Forwarding Connector

The ArcSight Forwarding Connector lets you receive events from a source Manager installation and send them to a secondary destination Manager, a non-ESM location or to an ArcSight Logger.

The ESM Source Manager is the installation from which events originate on a network using the ArcSight Forwarding Connector. The Forwarding Connector sends on (or "forwards") events to a destination Manager, a non-ESM location or a Logger appliance.

You can set up the Forwarding Connector after the First Boot Wizard completes. The Forwarding Connector is located in `/opt/arcSight/software/connector/forwardConnr/ArcSight-5.2.7.xxxx.0-SuperConnector-Linux64.bin`. For details on installing them, see the respective connector configuration guides for these connectors. See the ArcSight Forwarding Connector Configuration Guide for installation and configuration information for this connector.

## Update Connector Parameters

To update parameters for a specific connector, select the connector and click the edit icon next to the **Connector Parameters** link. Modify parameters as needed and click **Next**. Then, click **Done** when complete. The updated parameters are displayed in the **Connector Parameters** section of the Connector page.

For details, see "Editing Connector Parameters" in the Connector Management for ArcSight Express 4.0 User's Guide.

## Importing the Manager's Certificate

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

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

## Using keytoolgui to Import Manager's Certificate



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

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

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

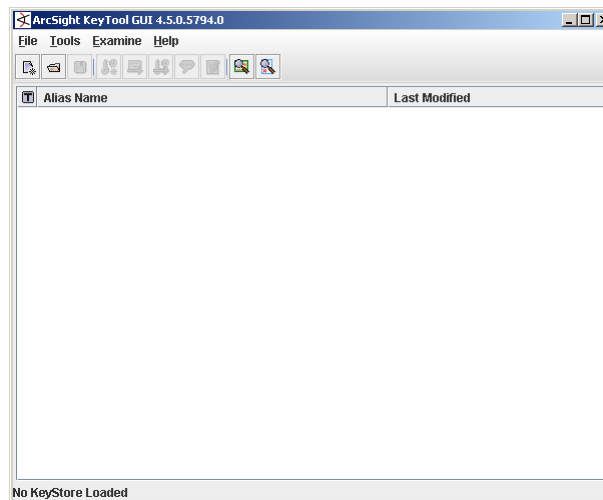
### Exporting the Manager's Certificate

To export the Manager's certificate:

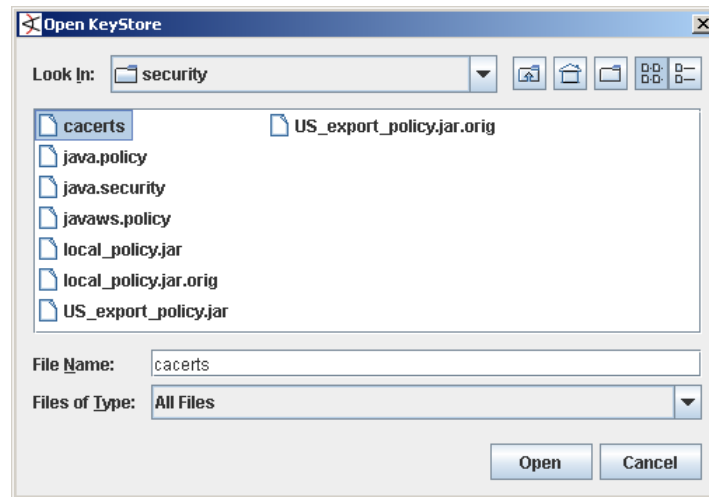
- 1 Open a shell window.
- 2 Run the following command from the Manager's `/opt/arcsight/manager/bin` directory while logged in as user "arcsight":

```
./arcsight keytoolgui
```

The keytoolgui interface will open.



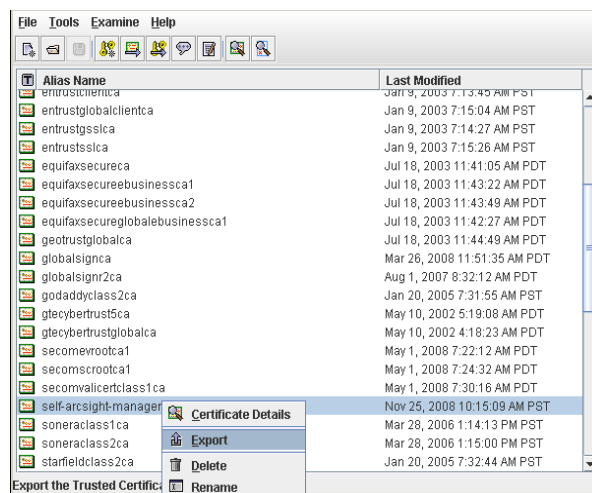
- 3 Select **File->Open KeyStore** from the menu and navigate to the Manager's truststore (cacerts) located in /opt/arcsight/manager/jre/lib/security/ directory.



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

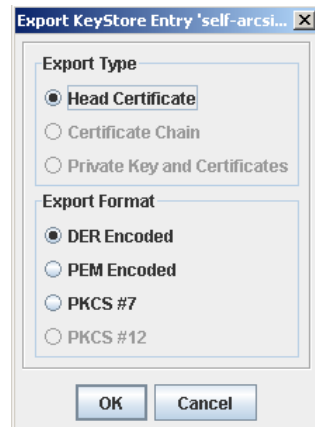


- 5 Right-click the Manager's certificate as shown below and select **Export**.

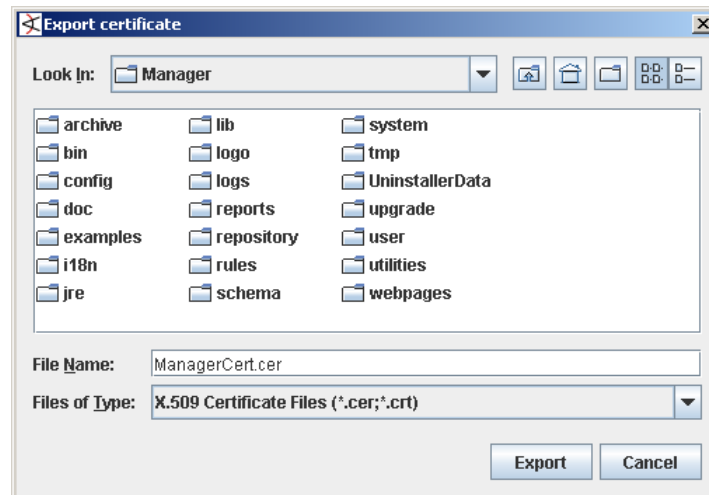




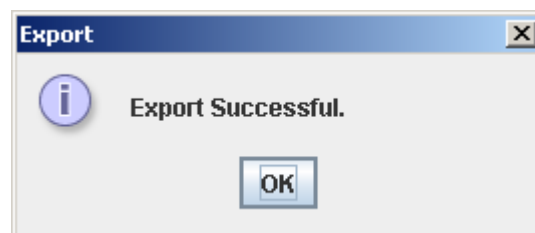
- 6 Accept the default settings in the following dialog and click **OK**.



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



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



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

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

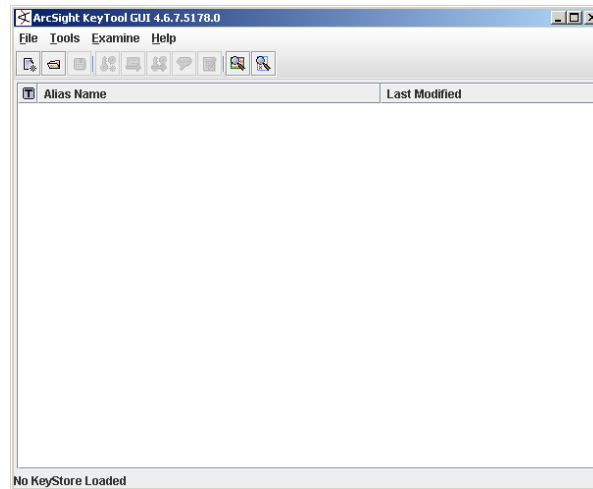
Import the certificate you exported above into the Connector's truststore.

To do so:

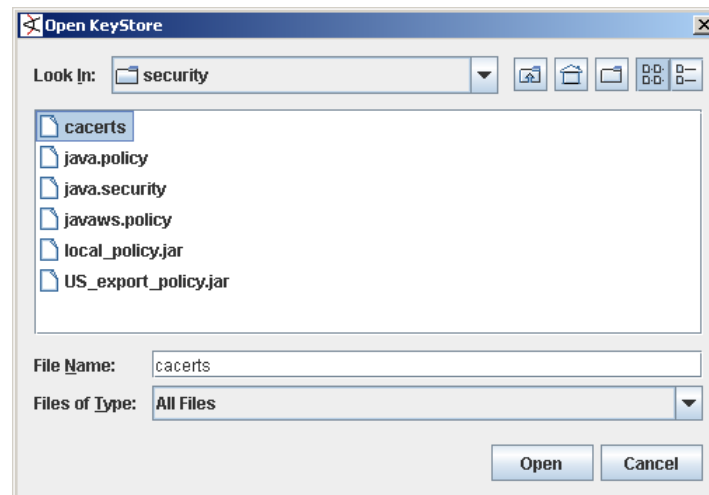
- 1 Open a shell window on the SmartConnector server.
- 2 While logged in as user "arcsight", run the following command from the Connector's bin directory (/home/arcsight/ArcSightSmartConnectors/current/bin on Unix and C:\arcsight\ArcSightSmartConnectors\current\bin on Windows):

```
./arcsight agent keytoolgui
```

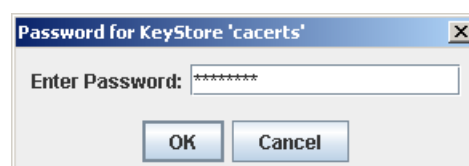
The keytoolgui interface will open.



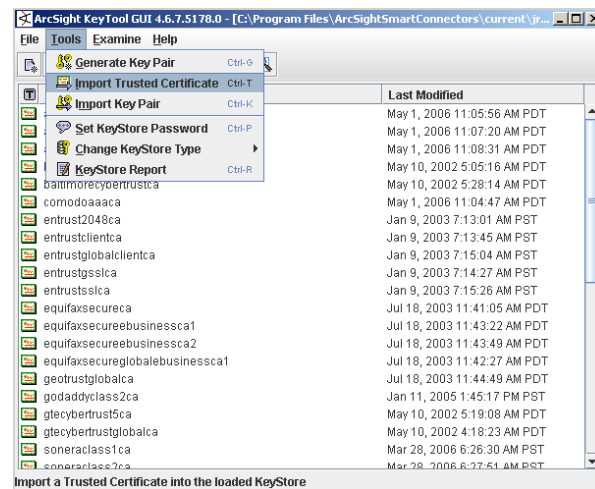
- 3 Select **File->Open KeyStore** from the menu and navigate to the Connector's truststore (cacerts) located in /home/arcsight/ArcSightSmartConnectors/current/jre/lib/security directory on Unix and C:\arcsight\ArcSightSmartConnectors\current\jre\lib\security on Windows.



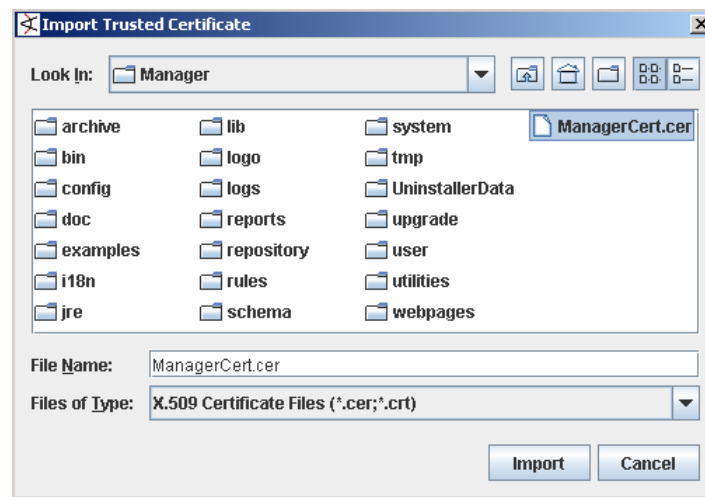
- 4 Enter the password. The default password is "changeit" (without the quotes).



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



6 Navigate to the Manager's certificate, select it and click **Import**.



7 You will see the following prompt. Click **OK** to see the certificate details.



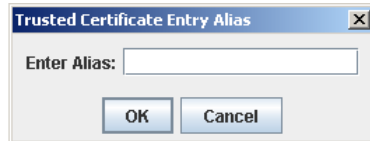
The **Certificate Details** dialog will be displayed.

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

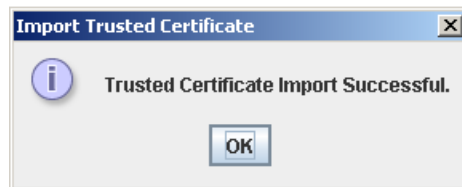
- 9 Click **Yes** in the following dialog.



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



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



- 12 Click **OK**.
- 13 Click **File->Save KeyStore** to save the certificate in the Connector's truststore and exit the keytoolgui interface.
- 14 Run the following from the connector's bin directory:

```
./runagentsetup
```

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

## Appendix A

# Troubleshooting

The following information may help solve problems that might occur when installing or using ArcSight Express. In some cases, the solution can be found here or in other ArcSight Express 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 69](#)  
["Customizing ArcSight Express Components Further" on page 71](#)  
["Fatal Error When Running the First Boot Wizard" on page 72](#)  
["Changing the IP Address of Your Machine" on page 73](#)  
["Changing the Host Name of the Machine After Running the First Boot Wizard" on page 74](#)

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

## Location of Log files for Components

The log files can be found in the following location:

Log file name	location	Description
<b>First Boot Wizard Logs</b>		
fbwizard.log	/opt/arcsight/manager/logs/default/	Contains detailed troubleshooting information logged during the steps when running the First Boot Wizard.
appliancefirstbootsetup.log	/opt/arcsight/manager/logs/	Contains brief troubleshooting information about commands that ran during the steps when running the First Boot Wizard.
<b>CORR-Engine Log Files</b>		

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_setup.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>ArcSight Manager Log Files</b>		
server.log	/opt/arcsight/manager/logs/default	Contains troubleshooting information about the ArcSight Manager
server.std.log	/opt/arcsight/manager/logs/default	Contains the stdout output of the ArcSight 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	ArcSight Manager status monitoring log file

Log file name	location	Description
<b>Log file for services</b>		
arcsight_services.log	/opt/arcsight/services/logs/	Contains information from commands that manage ArcSight service processes.
monit.log	/opt/arcsight/services/monit/data/	Contains timing information from startup and shutdown of ArcSight service processes.
<b>Log file for Connector Management Module</b>		
arcsight_logger.log	Access using the Send Logs Utility.	Connector Management Module service log.
conapp_init_driver.log	Access using the Send Logs Utility.	Installation log
conapp_wizard.out.log	Access using the Send Logs Utility.	Configuration wizard log
logger_web.log	Access using the Send Logs Utility.	Main Connector Management Module log file
logger_web.out.log	Access using the Send Logs Utility.	This is the stdout version of logger_web.log. It has more details such as GC, that goes to stdout but not the regular log.

For information on log files for connectors, refer to each connectors Configuration Guide.

## Customizing ArcSight Express Components Further

The First Boot Wizard allows you to configure the ArcSight Manager, SmartConnectors 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 ArcSight 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 ArcSight 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
```

### ArcSight SmartConnectors

Setting up the prebundled SmartConnectors in the First Boot Wizard is optional. You can optionally set them up at any time after the First Boot Wizard completes using the Connector Management tab on the Management Console.

## 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 69](#).

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 and UDP ports are open.
- 3 The First Boot Wizard can only be rerun if it did not reach the point where it configures the ArcSight Manager. 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 appliancefirstbootsetup -boxster -soft
```

In console mode:

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



## Changing the IP Address of Your Machine

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



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

**Note**

- 1 Log in as "root" and stop Connector 1 and Connector 2 by running the following commands:
 

```
/sbin/service arcsight_services stop connector_1
```

```
/sbin/service arcsight_services stop connector_2
```
- 2 Log out as *root* and log in again as user *arcsight*.
- 3 Stop all ArcSight services by running (as user "arcsight"):
 

```
/sbin/service arcsight_services stop all
```
- 4 Change the IP address of your machine.
- 5 Reboot the machine.
- 6 If running, stop the ArcSight Manager and ArcSight Web.
- 7 While logged in as user "arcsight", run the following to start the setup program for the ArcSight Manager from `/opt/arcsight/manager/bin` directory:
 

```
./arcsight managersetup
```

This will open the ArcSight Manager's setup wizard.

  - a Enter the new IP address (that you set for your machine in [Step 4](#) above) in the ArcSight 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.
- 8 Start the ArcSight Manager by running (as user "arcsight"):
 

```
/sbin/service arcsight_services start manager
```
- 9 Export the ArcSight 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.
- 10 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 4](#) 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.
- 11** Start ArcSight Web by running (as user “arcsight”):

```
/sbin/service arcsight_services start arcsight_web
```
- 12** Import the ArcSight Manager’s newly generated certificate on all clients (ArcSight Consoles and SmartConnectors) that will be accessing the ArcSight 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.
- 13** If not already started, start all components. You can do so by running (as user “arcsight”):

```
/sbin/service arcsight_services start all
```
- 14** Log in as “root” and start Connector 1 and Connector 2 by running the following commands:

```
/sbin/service arcsight_services start connector_1  
/sbin/service arcsight_services start connector_2
```
- 15** Test to make sure that the clients can connect to the ArcSight Manager.

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



Please note that the `managersetup` 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 Log in as "root" and stop Connector 1 and Connector 2 by running the following commands:  
  

```
/sbin/service arcsight_services stop connector_1
```

```
/sbin/service arcsight_services stop connector_2
```
- 2 Stop all services by running (as user "arcsight"):  
  

```
/sbin/service arcsight_services stop all
```
- 3 Change the host name of your machine.
- 4 Reboot the machine.

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

- 5 Stop the ArcSight Manager by running (as user "arcsight"):  

```
/sbin/service arcsight services stop manager
```

- 6 Stop ArcSight Web by running (as user "arcsight"):

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

- 7 While logged in as user "arcsight", run the ArcSight 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.

- 8 Start the ArcSight Manager by running (as user "arcsight"):

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

- 9 Export the ArcSight 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.

- 10 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.

- 11 Start ArcSight Web by running (as user "arcsight"):

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

- 12 Import the ArcSight Manager's certificate on all clients (ArcSight Consoles and SmartConnectors) that will be accessing the ArcSight 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.

- 13 If not already started, start all components. You can do so by running (as user "arcsight"):

```
/sbin/service arcsight_services start all
```

- 14 Log in as "root" and start Connector 1 and Connector 2 by running the following commands:

```
/sbin/service arcsight_services start connector_1
```

```
/sbin/service arcsight_services start connector_2
```

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

## The remote\_management.p12 file is empty

When the Microsoft Windows Event Log -Unified connector is not installed with First Boot Wizard, and the remote\_management.p12 file is empty due to some process being interrupted (process not completed) the Connector Manager Container N (where N is the container number) will appear to be down with the following error message:

```
Down : java.rmi.RemoteException: Could not download SSL Certificate
from the connector container with URL
https://localhost:9002/cwsapi/services/v1...
```

To work around this, remove the existing remote\_management.p12 file from the container, import the correct certificate for Connector Management. If Container N is down, execute the command:

```
/sbin/service arcsight_services start connector_N
```

and add the connector.

# Default Settings for Components

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

[“General” on page 77](#)

[“CORR-Engine” on page 77](#)

[“ArcSight Manager” on page 78](#)

[“ArcSight Web” on page 79](#)

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

## ArcSight Manager



**Note**

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

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

Setting	Default Value
Location of ArcSight Manager	/opt/arcsight/manager
ArcSight Manager host name	Host name or IP address of ArcSight Express
ArcSight Manager Port	8443
ArcSight 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 ArcSight Manager by running the following command (as user "arcsight"):</li> </ol> <pre>/sbin/service arcsight_services stop manager</pre> <ol style="list-style-type: none"> <li>2 Run the following command from the /opt/arcsight/manager/bin directory and set up the external SMTP server when prompted:</li> </ol> <pre>./arcsight managersetup</pre> <ol style="list-style-type: none"> <li>3 Start the ArcSight Manager by running (as user "arcsight"):</li> </ol> <pre>/sbin/service arcsight_services start manager</pre>
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 for you.

Setting	Default Value
Location of ArcSight Web	/opt/arcsight/web
ArcSight Web host name	Host name or IP address of ArcSight Express
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

## SmartConnectors

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

Setting	Default Value
<b>Forwarding Connector</b>	
Location of binary file	/opt/arcsight/software/connector/forwardConnr/ArcSight-5.2.7.xxx.0-SuperConnector-Linux64.bin
Location of log files	/opt/arcsight/software/connector/forwardConnr/current/logs
Port number	8443
<b>ArcSight Reputation Security Monitor Model Import Connector</b>	
Location of binary file	/opt/arcsight/software/connector/repSmConnr/ArcSight-5.2.7.xxx.0-RepSMMModelConnector-Linux64.bin
Location of log files	/opt/arcsight/software/connector/repSmConnr/current/logs
Port number	443 by default
<b>Syslog Daemon Connector</b>	

Setting	Default Value
Location of installation file and where it will be installed	/opt/arcsight/connector_n where n is the container number; connector_1 or connector_2 when installed using the First Boot Wizard. If you install it after the First Boot Wizard completes, it could be any of the containers.
By default, installed in	/opt/arcsight/connector_n/current where n is the container number; connector_1 when installed using the First Boot Wizard. If you install it after the First Boot Wizard completes, it could be any of the containers.
Port number	514 by default
Location of log files	/opt/arcsight/connector_1/current/ logs
<b>Microsoft Windows Event Log - Unified connector</b>	
Location of installation file and where it will be installed	/opt/arcsight/connector_n where n is the container number; connector_1 or connector_2 when installed using the First Boot Wizard. If you install it after the First Boot Wizard completes, it could be any of the containers.
By default, installed in	/opt/arcsight/connector_n/current where n is the container number; connector_2 when installed using the First Boot Wizard. If you install it after the First Boot Wizard completes, it could be any of the containers.
Location of log files	/opt/arcsight/connector_n/current/ logs



## Appendix C

# About Locales and Encodings

---

The software on ArcSight Express is translated into various languages, for instance English, French, Japanese, and traditional Chinese. Setting the Locale for any of these languages ensures that you get the appropriate environment in terms of language settings, number format, date/time format, timezone settings, and Daylight Saving Time setting for that country or language. This appendix describes the updates to be taken into consideration when configuring ArcSight Express for a supported language.

This appendix covers the following topics:

["Terminology" on page 81](#)

["Before you Install a Localized Version of ArcSight Express" on page 82](#)

["Localization of Date Formats in Tokens and Operations" on page 84](#)

["Key-Value Parsers for Localized Devices" on page 84](#)

["List of possible values for the agent.parser.locale.name property" on page 85](#)

["List of possible values for the agent.parser.locale.name property" on page 85](#)

## Terminology

Some of the common terms used in this document are described below.

### Internationalization

Internationalization is the process of designing an application so that it can be adapted to various languages and regions without further engineering changes.

### Locale

Locale refers to the specific language of the region where you are running ArcSight Express.

### Character Set

A character set is a collection of characters that have been grouped together for a particular purpose. An example of a character set is the English alphabet.

### Code Set

Each character in a character set is assigned a unique value. Collectively, these values are known as a code set.

## Code Point

Each character value within a code set is referred to as a code point.

## Encoding

Encoding specifies how each character's code point is stored in memory or disk files.

## Unicode

Unicode is a universal character set that assigns a unique code point to characters from all major languages of the world.

## Before you Install a Localized Version of ArcSight Express

Keep in mind that the ArcSight Manager and ArcSight Console should all be configured with the same locale.

By default, all communication between the ArcSight Express components is done using UTF-8 character encoding. Even though ArcSight Express supports only UTF-8 internally, if your Connector receives events in UTF-16, for example, the events are still stored correctly since these events get converted to UTF-8 by the Connector before they are passed on to the ArcSight Manager. The ArcSight Manager then passes these events to the database where they are persisted in UTF-8.



Caution

### On Windows only:

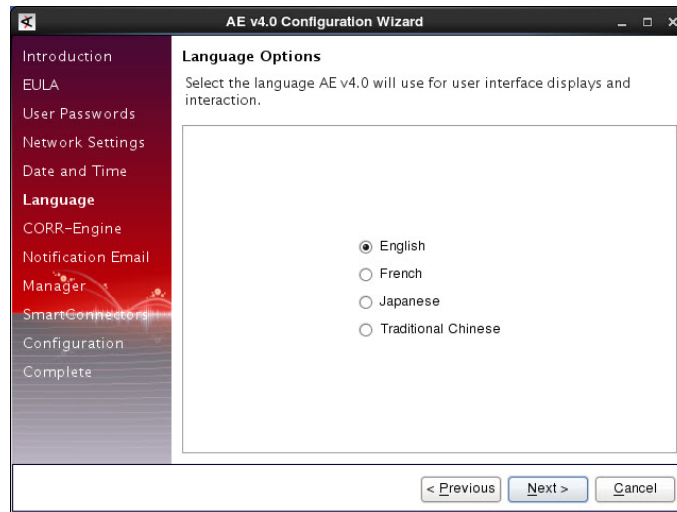
If your Operating System was installed in a particular locale, but you changed the locale later on your desktop environment to another language, the locale that was set during the OS installation will take precedence for the applications that run as a service. For instance, in such a scenario, ArcSight SmartConnectors running as a service will adopt the locale in which the operating system was installed.

To work around this, edit the service settings for the webserver and change it to run as the user who changed the locale on the desktop. This will allow you to view the application in the locale that was set on your desktop environment.

To change the settings for a service,

- 1 Right click the service and select **Properties**.
  - 2 Click the **Logon** tab.
  - 3 Select **This account** and browse to the user account that had changed the locale and enter that account's password.
  - 4 Click **OK**.
-

During startup, ArcSight Express automatically detects and uses the locale from the Operating System. You can set up the locale of your choice in the following First Boot Wizard panel.



## ArcSight Console

Install the ArcSight Console on an Operating System that is of the same language as the language you selected while setting up ArcSight Express. During startup, ArcSight Console automatically detects and uses the locale from the Operating System.

## ArcSight SmartConnectors

If a device is configured to use a language-specific encoding (not Unicode), the Connector receiving events from this device should be configured to use the same encoding as the device.

### Setting the Encoding for Selected SmartConnectors

You can set the encoding to a character set corresponding to your locale for the following SmartConnectors only:

- SAP Real-Time Security Audit Multi-Folder Connector.  
See the SmartConnector for SAP Real-time Security Audit Multi-Folder Configuration Guide for instructions on how to configure the encoding for this Connector.
- IBM DB2 Audit File Connector.  
See the SmartConnector for IBM DB2 Audit File Configuration Guide for instructions on how to configure the encoding for this Connector.
- Oracle SYSDBA Audit Multi-Folder Connectors  
See the SmartConnector for Oracle SYSDBA Audit Multi-Folder Configuration Guide for instructions on how to configure the encoding for this Connector.

The above SmartConnectors support all character sets supported by Java.



You need to change the encoding to match the log files' encoding only if the log files use an encoding other than the default one.

Connectors not mentioned above use the default encoding of the Operating System on which they reside. Each Operating System comes with default encodings for various languages of the world. So, the encoding used in a Connector is either based on the character set that you selected in the First Boot Wizard or the Operating System you are using.

## Localization of Date Formats in Tokens and Operations

If your Connector receives logs that contain timestamps in a non-English language or a date format that is customarily used by a non-English locale (for example, "mai 24, 2006 12:56:07.615" where "mai" is German for May), configure the `agent.parser.locale.name` property in the `agent.properties` file. This file is located in `ARCSIGHT_HOME/current/user/agent` directory.

Set the `agent.parser.locale.name` property to the value that corresponds to the Connector's locale. By default, this property is set to `en_US`. Refer to the table at the end of this document under section "List of possible values for the `agent.parser.locale.name` property" for possible values for this property.

## Key-Value Parsers for Localized Devices

Some localized devices not only send localized Values but also localized Keys in event messages. In such a case, additional processing may be needed to translate the Keys to English for the event messages to be properly parsed. For example, assume that the content of a key-value parser is:

`event.destinationUserName=User`

And the received event message is:

User= 田中 where 田中 is Japanese for TANAKA.

In that case, the parser as it is works fine since double byte is supported already.

If the received event message is:

ユーザ = 田中 where ユーザ is Japanese for User.

Then additional mapping is needed to translate ユーザ to User.

If you encounter a need for a localized device, please contact Customer Support using the HP SSO website.

Windows Event Log Connector supports the following locales to parse the non-English language Keys in the Windows Event Log description:

- ja (Japanese)
- de (German)
- zh\_CN (Simplified Chinese)
- zh\_TW (Traditional Chinese)

Please call Customer Support for assistance with other non-supported languages.

## Examples

The following examples cover two different scenarios.

### Scenario 1 - Events received in a single language only

This scenario describes what you need to do when your Connector(s) receive data in a single language only, for instance Japanese. In ArcSight Express, the default encoding for Japanese is JA16SJIS.

#### First Boot Wizard

While installing ArcSight Express, select Japanese from the list in the Languages panel.

#### ArcSight Manager, ArcSight Console, and ArcSight Web

On startup, the ArcSight Manager, ArcSight Console, and ArcSight Web automatically pick up and use the locale from the Operating System. So, if the Red Hat Linux on your appliance is set to Japanese, on startup, these components automatically pick up and use the Japanese locale from the Operating System.

### Scenario 2 - Events received in multiple languages

This scenario is an example of what you need to do when you are dealing with multiple Connectors that receive data in different languages.

#### First Boot Wizard

When running the First Boot Wizard, select the language in which you want the standard content resources to be installed.

#### ArcSight Manager, ArcSight Console, and ArcSight Web

In the First Boot Wizard, you selected a language in which to install the system resources. Make sure that the Red Hat Linux has been set to the same language. On startup, the ArcSight Manager, ArcSight Console, and ArcSight Web automatically pick up the locale from the Operating System.

## List of possible values for the agent.parser.locale.name property

The table below lists the possible values for this property.

Values	Language	Country	Variant
ar	Arabic		

Values	Language	Country	Variant
ar_AE	Arabic	United Arab Emirates	
ar_BH	Arabic	Bahrain	
ar_DZ	Arabic	Algeria	
ar_EG	Arabic	Egypt	
ar_IQ	Arabic	Iraq	
ar_JO	Arabic	Jordan	
ar_KW	Arabic	Kuwait	
ar_LB	Arabic	Lebanon	
ar_LY	Arabic	Libya	
ar_MA	Arabic	Morocco	
ar_OM	Arabic	Oman	
ar_QA	Arabic	Qatar	
ar_SA	Arabic	Saudi Arabia	
ar_SD	Arabic	Sudan	
ar_SY	Arabic	Syria	
ar_TN	Arabic	Tunisia	
ar_YE	Arabic	Yemen	
be	Belarusian		
be_BY	Belarusian	Belarus	
bg	Bulgarian		
bg_BG	Bulgarian	Bulgaria	
ca	Catalan		
ca_ES	Catalan	Spain	
cs	Czech		
cs_CZ	Czech	Czech Republic	
da	Danish		
da_DK	Danish	Denmark	
de	German		
de_AT	German	Austria	
de_CH	German	Switzerland	
de_DE	German	Germany	
de_LU	German	Luxembourg	
el	Greek		
el_GR	Greek	Greece	

Values	Language	Country	Variant
en	English		
en_AU	English	Australia	
en_CA	English	Canada	
en_GB	English	United Kingdom	
en_IE	English	Ireland	
en_IN	English	India	
en_NZ	English	New Zealand	
en_US	English	United States	
en_ZA	English	South Africa	
es	Spanish		
es_AR	Spanish	Argentina	
es_BO	Spanish	Bolivia	
es_CL	Spanish	Chile	
es_CO	Spanish	Columbia	
es_CR	Spanish	Costa Rica	
es_DO	Spanish	Dominican Republic	
es_EC	Spanish	Ecuador	
es_ES	Spanish	Spain	
es_GT	Spanish	Guatemala	
es_HN	Spanish	Honduras	
es_MX	Spanish	Mexico	
es_NI	Spanish	Nicaragua	
es_PA	Spanish	Panama	
es_PE	Spanish	Peru	
es_PR	Spanish	Puerto Rico	
es_PY	Spanish	Paraguay	
es_SV	Spanish	El Salvador	
es_UY	Spanish	Uruguay	
es_VE	Spanish	Venezuela	
et	Estonian		
et_EE	Estonian	Estonia	
fi	Finnish		
fi_FI	Finnish	Finland	
fr	French		

Values	Language	Country	Variant
fr_BE	French	Belgium	
fr_CA	French	Canada	
fr_CH	French	Switzerland	
fr_FR	French	France	
fr_LU	French	Luxembourg	
hi_IN	Hindi	India	
hr	Croatian		
hr_HR	Croatian	Croatia	
hu	Hungarian		
hu_HU	Hungarian	Hungary	
is	Icelandic		
is_IS	Icelandic	Iceland	
it	Italian		
it_CH	Italian	Switzerland	
it_IT	Italian	Italy	
iw	Hebrew		
iw_IL	Hebrew	Israel	
ja	Japanese		
ja_JP	Japanese	Japan	
ko	Korean		
ko_KR	Korean	Korea	
lt	Lithuanian		
lt_LT	Lithuanian	Lithuania	
lv	Latvian		
lv_LV	Latvian	Latvia	
mk	Macedonian		
mk_MK	Macedonian	Macedonia	
nl	Dutch		
nl_BE	Dutch	Belgium	
nl_NL	Dutch	Netherlands	
no	Norwegian		
no_NO	Norwegian	Norway	
no_NO_NY	Norwegian	Norway	Nynorsk
pl	Polish		



Values	Language	Country	Variant
pl_PL	Polish	Poland	
pt	Portuguese		
pt_BR	Portuguese	Brazil	
pt_PT	Portuguese	Portugal	
ro	Romanian		
ro_RO	Romanian	Romania	
ru	Russian		
ru_RU	Russian	Russia	
sk	Slovak		
sk_SK	Slovak	Slovakia	
sl	Slovanian		
sl_SI	Slovanian	Slovania	
sq	Albanian		
sq_AL	Albanian	Albania	
sv	Swedish		
sv_SE	Swedish	Sweden	
th	Thai		
th_TH	Thai	Thailand	
th_TH_TH	Thai	Thailand	TH
tr	Turkish		
tr_TR	Turkish	Turkey	
uk	Ukranian		
uk_UA	Ukranian	Ukraine	
vi	Vietnamese		
vi_VN	Vietnamese	Vietnam	
zh	Chinese		
zh_CN	Chinese	China	
zh_HK	Chinese	Hong Kong	
zh_TW	Chinese	Taiwan	



## Appendix D

# Using the PKCS#11 Token

---

This appendix covers the following topics:

[“What is PKCS?” on page 91](#)

[“PKCS#11 Token Support in ArcSight Express” on page 92](#)

[“References to <ARCSIGHT\\_HOME>” on page 92](#)

[“Setting Up to Use a CAC Card” on page 92](#)

[“Logging in to the Management Console Using CAC” on page 100](#)

[“Using CAC with ArcSight Web” on page 101](#)

ArcSight Express 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. ArcSight Express 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 ArcSight Express

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

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

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

- 1 Log in to the Management Console.
- 2 Go to the **Administration** tab.
- 3 Select **Configuration Management**, on the left.
- 4 Select **Authentication Configuration**.
- 5 Select **Password or SSL Client Based** authentication.
- 6 Restart the 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 Management Console, you can edit the External ID to match the common name on the Admin tab.

## References to <ARCSIGHT\_HOME>

<ARCSIGHT\_HOME> in the paths represents

- /opt/arcsight/manager for the 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 ArcSight Express supports authentication through any PKCS#11 token, this appendix covers how to use the ActivClient's Common Access Card (CAC) as an example.

### Install the CAC Provider's Software

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

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



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.

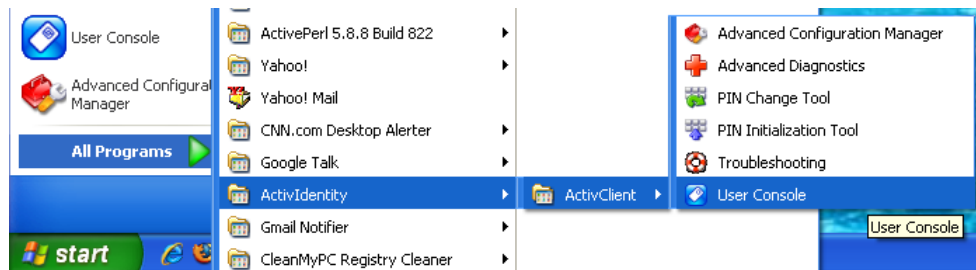
## Map a User's External ID to the CAC's Subject CN

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

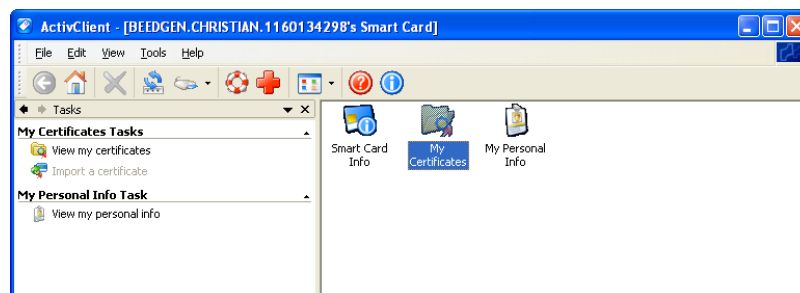
Map the Common Name (CN) on the CAC to a User's External ID on the ArcSight Manager. The external user ID must be identical to the Common Name that appears in the CAC card's ID certificate (include any spaces and periods that appear in the Common name). This allows the ArcSight Manager to know which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

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

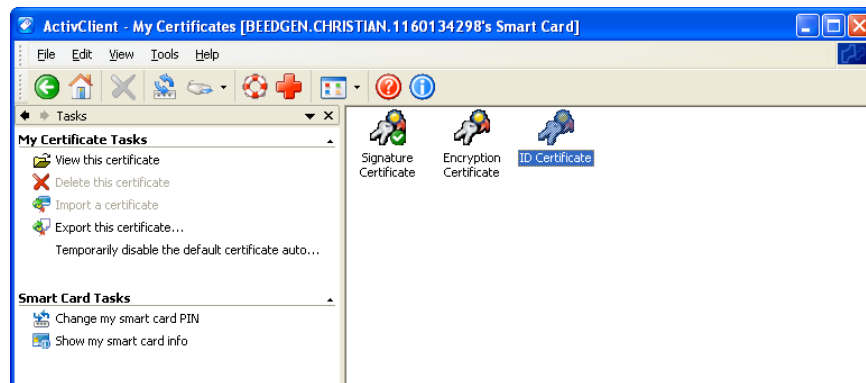
- 1 Obtain the Subject CN from the CAC card.
  - a Insert the CAC card into the reader if not already inserted.
  - b Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



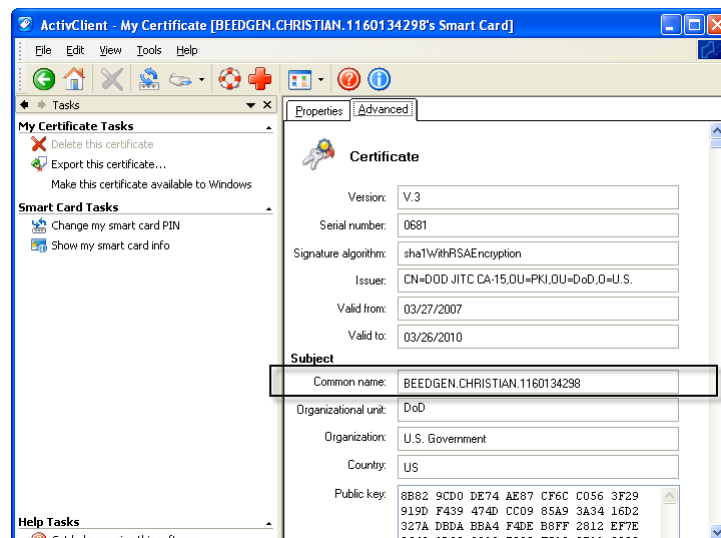
- c Double-click **My Certificates** in the following screen:



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



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



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

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

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

## Obtain the CAC's Issuers' Certificate

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

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

### Option 1:

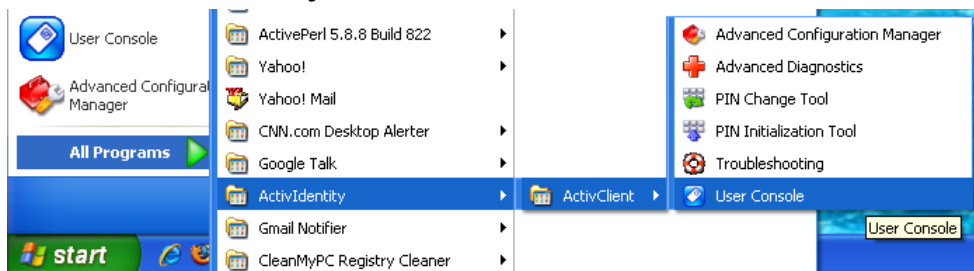
You can obtain the CAC card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

### Option 2:

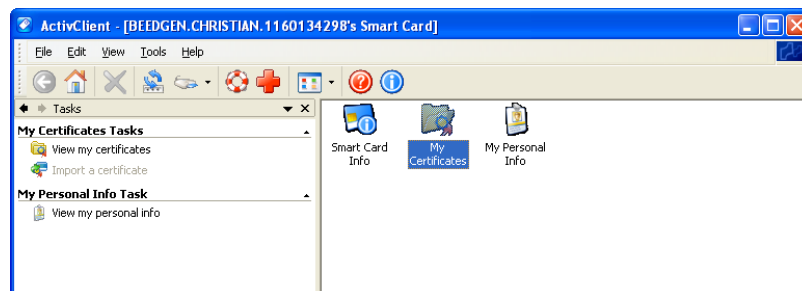
You can export the CAC card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

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

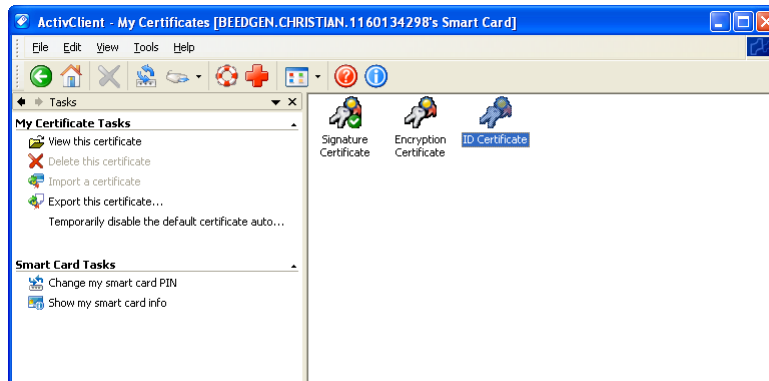
- 1 Insert the CAC card into the reader if not already inserted.
- 2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



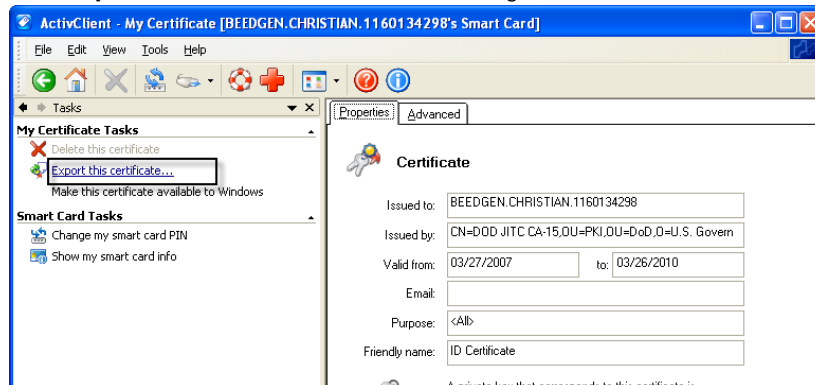
- 3 Double click **My Certificates** in the following screen:



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



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



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

## Extract the Root CA Certificate From the CAC Certificate

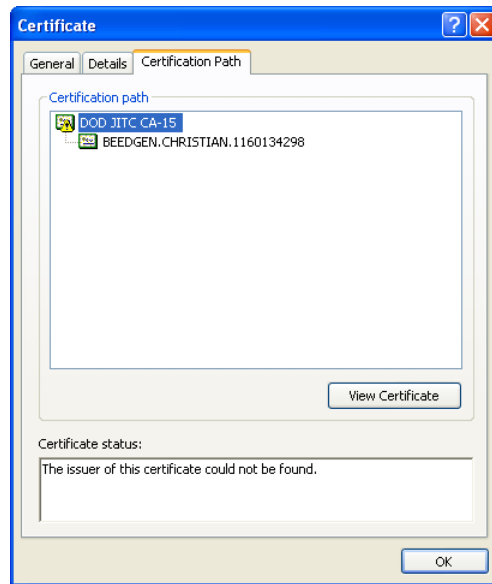
The CAC certificate signer's CA root certificate and any intermediate signers' certificate(s) have to be imported into the ArcSight Manager's `nssdb` (in FIPS mode) or `truststore` (in default mode).

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

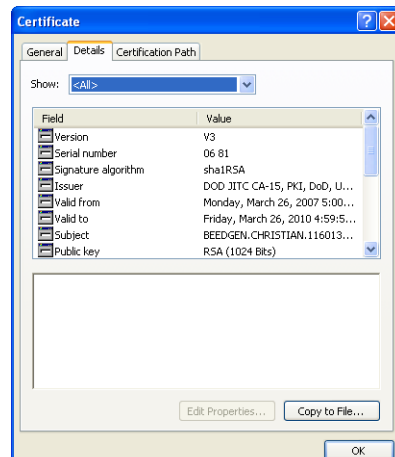
- 1 Double-click the CAC's certificate that you exported. The Certificate interface will open.



- 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:

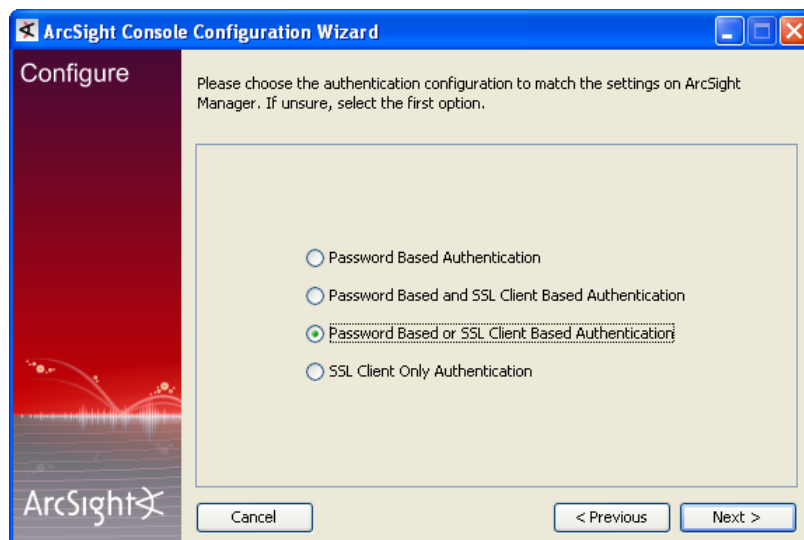
```
/sbin/service arcsight_services start manager
```

## Select Authentication Option in ArcSight Console Setup

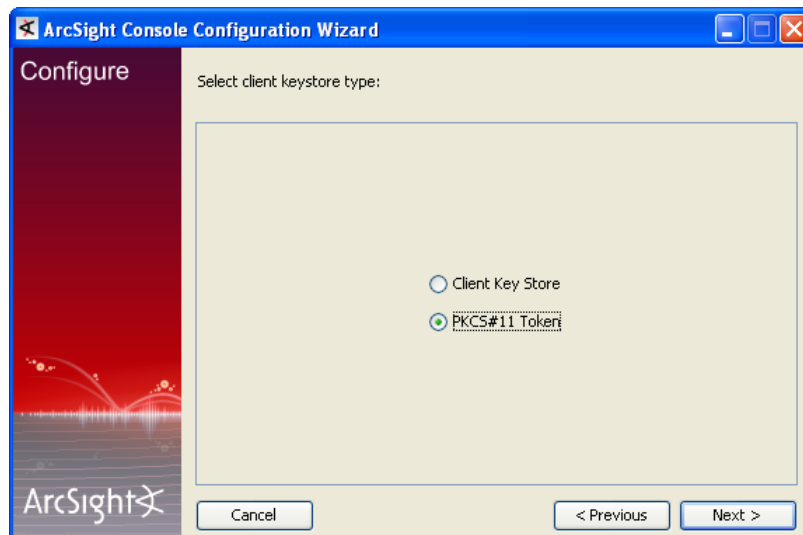
The authentication option on the ArcSight Console should match the authentication option that you set on the ArcSight Manager. Run the ArcSight Console setup program and either confirm or change the authentication on the ArcSight Console to match that of the ArcSight Manager. To do so:

- 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.

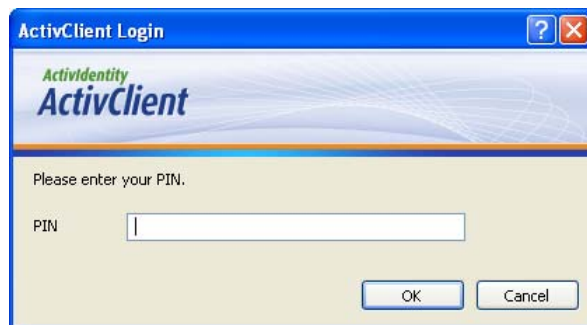
## Logging in to the ArcSight Console Using CAC

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.

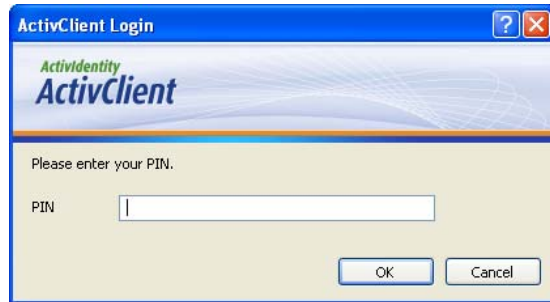


## Logging in to the Management Console Using CAC

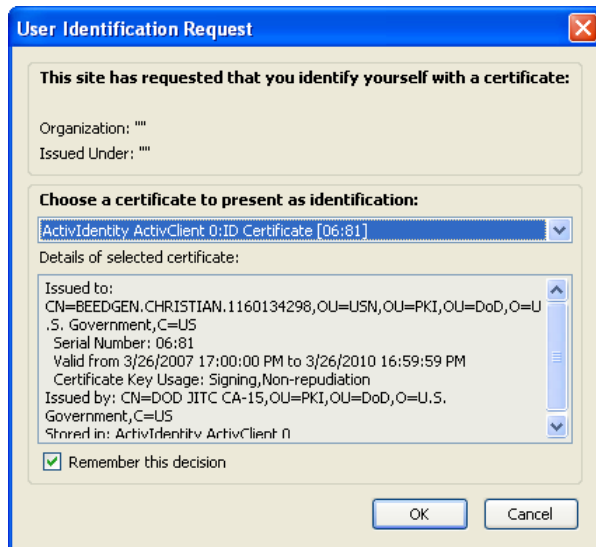
Use a supported web browser such as Firefox or Internet Explorer to connect to the Management Console.

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

- 3 You will be requested to enter your PIN



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



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

## Using CAC with ArcSight Web

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



## Appendix E

# ArcSight Express in FIPS Mode

---

This section covers the following topics:

- [“What is FIPS?” on page 103](#)
- [“Network Security Services Database \(NSS DB\)” on page 104](#)
- [“What is Suite B?” on page 104](#)
- [“NSS Tools Used to Configure Components in FIPS Mode” on page 105](#)
- [“TLS Configuration in a Nutshell” on page 105](#)
- [“Using PKCS #11 Token With a FIPS Mode Setup” on page 107](#)
- [“Installing ArcSight Console in FIPS Mode” on page 108](#)
- [“Configure Your Browser for FIPS” on page 112](#)
- [“Installing SmartConnectors in FIPS mode” on page 115](#)
- [“How do I Know If My Installation is FIPS Enabled?” on page 116](#)

ArcSight Express 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 ArcSight Express 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 ArcSight Express. 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 ArcSight Express versions support the FIPS with Suite B mode. Refer to the ArcSight Express Product Lifecycle Document available on the Protect 724 website for supported platforms for FIPS with Suite B mode.
  - When the ArcSight Express 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 ArcSight Express must be FIPS enabled.
  - Before installing ArcSight Express 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, ArcSight Express 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. ArcSight Express 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 ArcSight Express 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 211](#) 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 D, Using the PKCS#11 Token, on page 91](#).

- 1 Install the CAC provider's software on each client machine. That includes the ArcSight Console and every machine using a browser to access ArcSight Web or the Management Console. See ["Install the CAC Provider's Software" on page 92](#).
- 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.

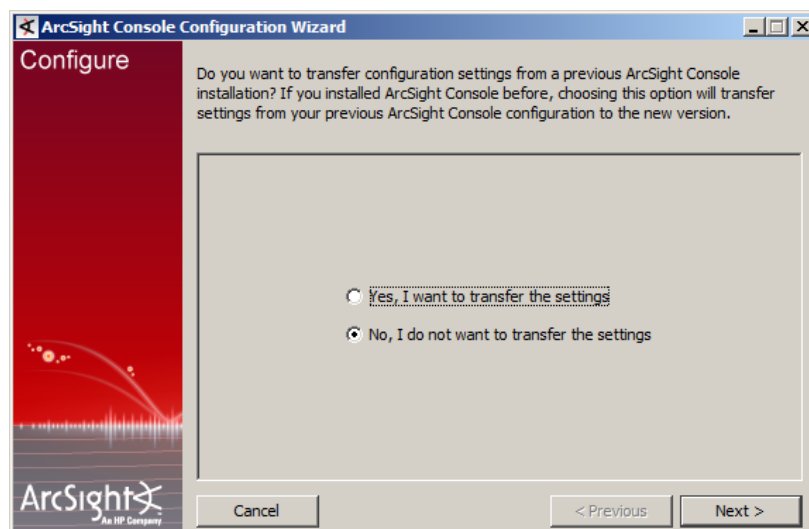
Refer to the ArcSight Express Product Lifecycle document available on the Protect 724 website (<https://protect724.arcsight.com>) for details on supported platforms for the ArcSight Console.

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.

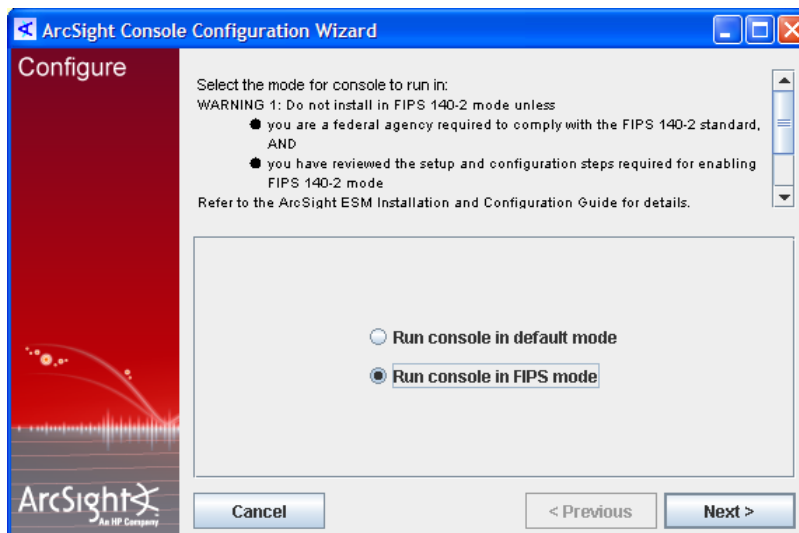
In order for an ArcSight Console to communicate with a FIPS enabled ArcSight Manager, the ArcSight Console must trust the ArcSight Manager. This trust is established by importing the ArcSight Manager's certificate into the ArcSight Console's NSS DB (<ARCSIGHT\_HOME>/current/config/nssdb.client). After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

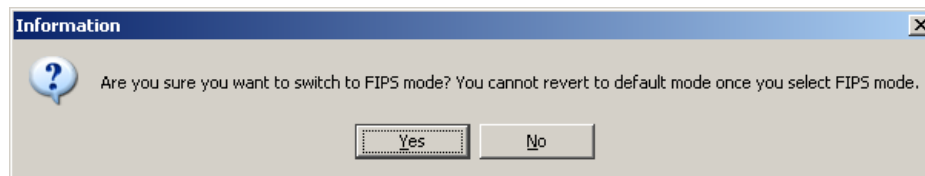


**Note**

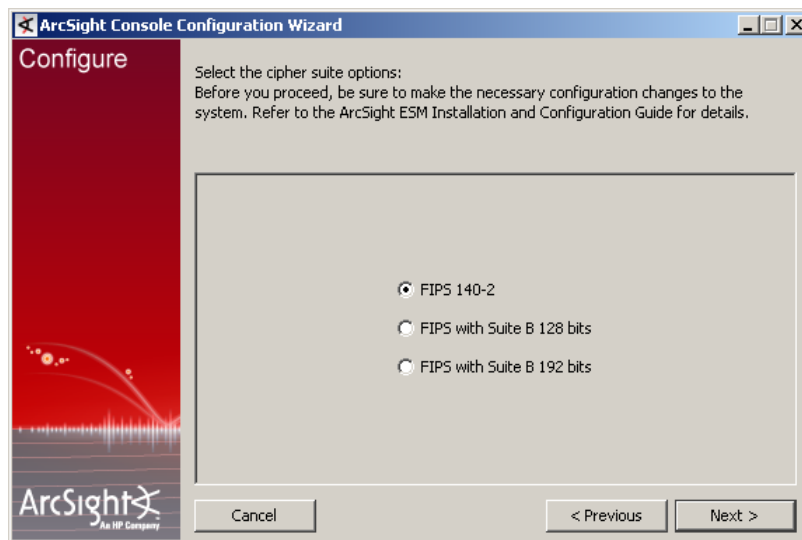
On the Windows XP, SP2 platform, you may see an error asking you to check the certificates in the NSSDB even though you have followed the steps to import the ArcSight Manager's certificate into the NSSDB successfully. If you encounter this error:

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

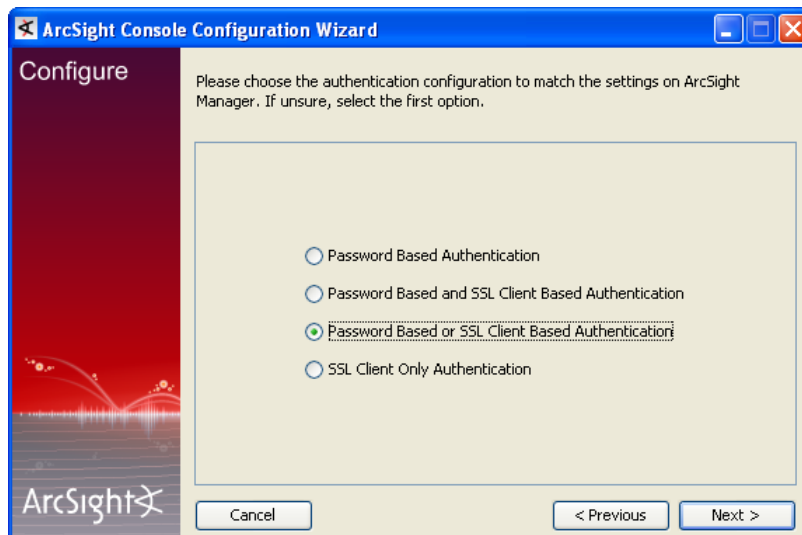
- 5 You will be reminded that once you select the FIPS mode, you will not be able to revert to the default mode. Click **Yes**.



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

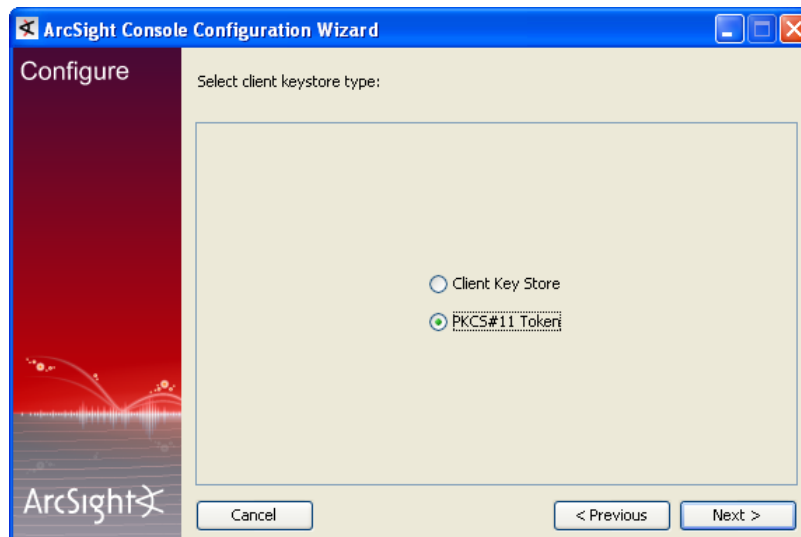


- 7 Next you will be prompted for the ArcSight Manager's hostname and port. The ArcSight Manager hostname must be the same (short name, fully qualified domain name, or IP address) as the Common Name (CN) you used when you created the ArcSight Manager key pair.
- 8 Follow the prompts in the next few wizard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

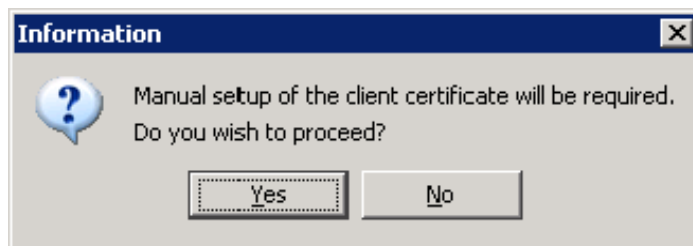
On 32-bit Windows:

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

On 64-bit Windows:

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

If you do not plan to use a PKCS #11 token with the 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 Management Console.

### FIPS with Firefox

FIPS can be configured for versions of Firefox up to version 14. The steps for Firefox are more involved than for other browsers, so they are included here.

- 1 In the Firefox window, select **Tools->Options...** (or **Edit->Preferences** in the case of Firefox on Linux)



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

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

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

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

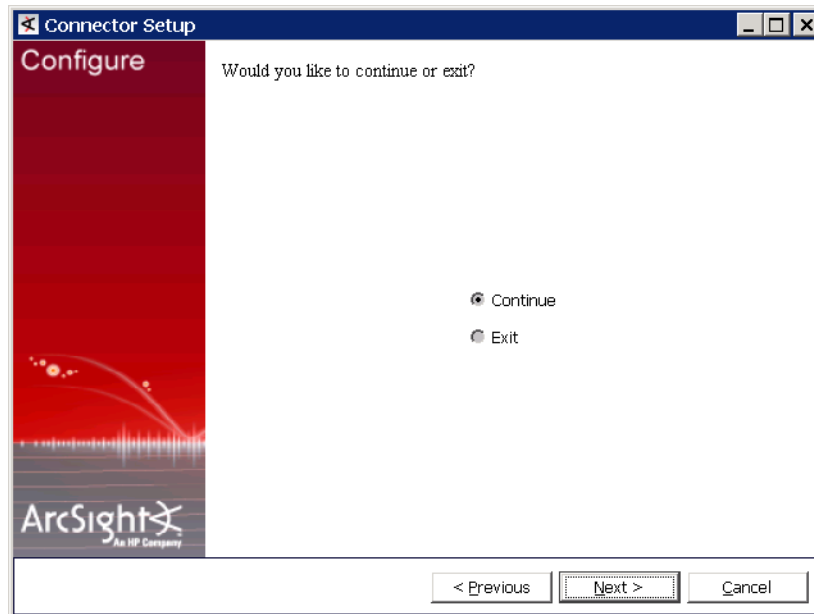
**16** Disable the TLS Ticket Extension as follows:

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

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

## 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 the "Exit" and click **Next** to quit the installation. You have to import the ArcSight Manager's certificate to allow the connector to trust the ArcSight Manager before adding a new connector.



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

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

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

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

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

Run `runagentsetup` to resume your connector setup.

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

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

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

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

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`.

## Appendix F

# Restoring Factory Settings

---

You can restore the ArcSight Express appliance to its original factory settings using the built-in System Restore utility.



Factory reset **irrevocably deletes all event and configuration data.**

Restoring ArcSight Express to factory settings will permanently delete all event data and configuration settings. If necessary, work with your HP Customer Support representative for ArcSight products before proceeding.

### To restore to its original factory settings:

- 1 Attach a keyboard, monitor, and mouse directly to the appliance.
- 2 Reboot the appliance from the GUI by selecting **System > Shut down**, then select **Restart**.
- 3 Immediately press any key when the screen displays this prompt:

```
Press any key to enter the menu
Booting Red Hat Enterprise Linux Server in 2 seconds ...
```



The prompt is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance continues to boot normally.

- 4 Use the mouse or arrow keys to select **System Restore (B1311)** and press **Enter**.

System Restore automatically detects and displays the archive image.

```
2013-03-22_B7400_B1311.ari
```

The image is named following this pattern:

```
YYYY-MM-DD_B7400_<build#>.ari
```

where YYYY-MM-DD is the date, B7400 is the appliance model, and build# is the build number of the image being restored.



If you encounter any issues with the image, contact HP ArcSight Customer Support.

- 5 Press **F10** (VERIFY) to check the archive for damage before performing the restore.
- 6 Press **F1** (AUTOSELECT) to automatically map the source image.

**7** Press **F2** (RESTORE) to begin the restore process.

**8** Press **y** to continue.

Progress bars show the status of the restoration.



Do not interrupt or power-down the ArcSight Express appliance during the restore process. Interrupting the restore process may force the system into a state from which it cannot be recovered.

---

**9** When the restore process is completed, press **F12** to reboot the appliance.

# Index

---

## A

- access control list (ACL) 33
- Active Directory, setting up authentication for 34
- appendix
  - example of 91, 103
- ArcSight
  - Manager 8
- ArcSight Console
  - client authentication 45
  - connecting to the Manager 42
  - installing 37, 39
  - reconfiguring 53
  - reconnecting to Manager 52
  - starting 50
  - uninstalling 53
  - user logs and preferences 48
  - web browser configuration 47
- ArcSight Express
  - Restore Factory Settings 117
- ArcSight Express Appliance
  - deployment overview 9
- ArcSight Express appliance
  - communication overview 9
  - configuring 13, 27
  - deployment overview 9
  - effects of communication when components fail 10
  - pre-installed software 7
  - restarting wizard 16
- ArcSight Manager
  - default settings 78
- authentication 32
  - Active Directory 34
  - built-in 33
  - custom JAAS plug-in configuration 35
  - external 32
  - LDAP 35
  - password-based 33
  - PKCS#11 32
  - RADIUS 33
  - SSL client-only 36

## B

- built-in authentication 33

## C

- changing
  - host name 74
  - IP address 73
- character set 40

- client authentication
  - ArcSight Console 45
- client keystore 36
- configuration
  - web browser in Console 47
- configuring
  - ArcSight Express appliance 13
  - SSL 34
- connecting
  - ArcSight Console to Manager 42
- Console
  - installing 39
  - supported platforms 37
- custom authentication scheme 35
- customizing
  - components 71

## D

- default settings
  - ArcSight Manager 78

## E

- ESM
  - overview 7
- external authentication 32
  - guidelines 32

## F

- factory settings
  - restore 117
- First Boot Wizard
  - fatal error 72

## H

- host name, changing 74
- hot key issue 40

## I

- installing
  - ArcSight Console 39
- IP address, changing 73

## J

- JAAS plug-in authentication 35

## **L**

### **LDAP**

- setting up authentication for 35

## **M**

### **Manager 8**

- transferring configuration 41

## **O**

### **overview**

- ArcSight Express Appliance communication 9
- ArcSight Express Appliance deployment 9

## **P**

- password-based authentication 33

### **passwords**

- character set 40

- PKCS#11 authentication 32

### **preferences**

- ArcSight Console 48

### **Pre-installed software**

- ArcSight Express Appliance 7

## **R**

### **RADIUS**

- setting up authentication for 33

### **reconfiguring**

- ArcSight Console 53

### **reconnecting**

- Console to Manager 52

### **restarting**

- ArcSight Express Appliance wizard 16

## **S**

- shortcut key issue 40

- SmartConnectors 55

### **SSL**

- client-only authentication 36

- configuring 34, 35

### **starting**

- ArcSight Console 50

- supported platforms

- Console 37

## **T**

### **Troubleshooting 69**

- fatal error 72

## **U**

### **uninstalling**

- ArcSight Console 53

### **user logs**

- ArcSight Console 48

## **W**

### **Web browser**

- configuring in Console 47