

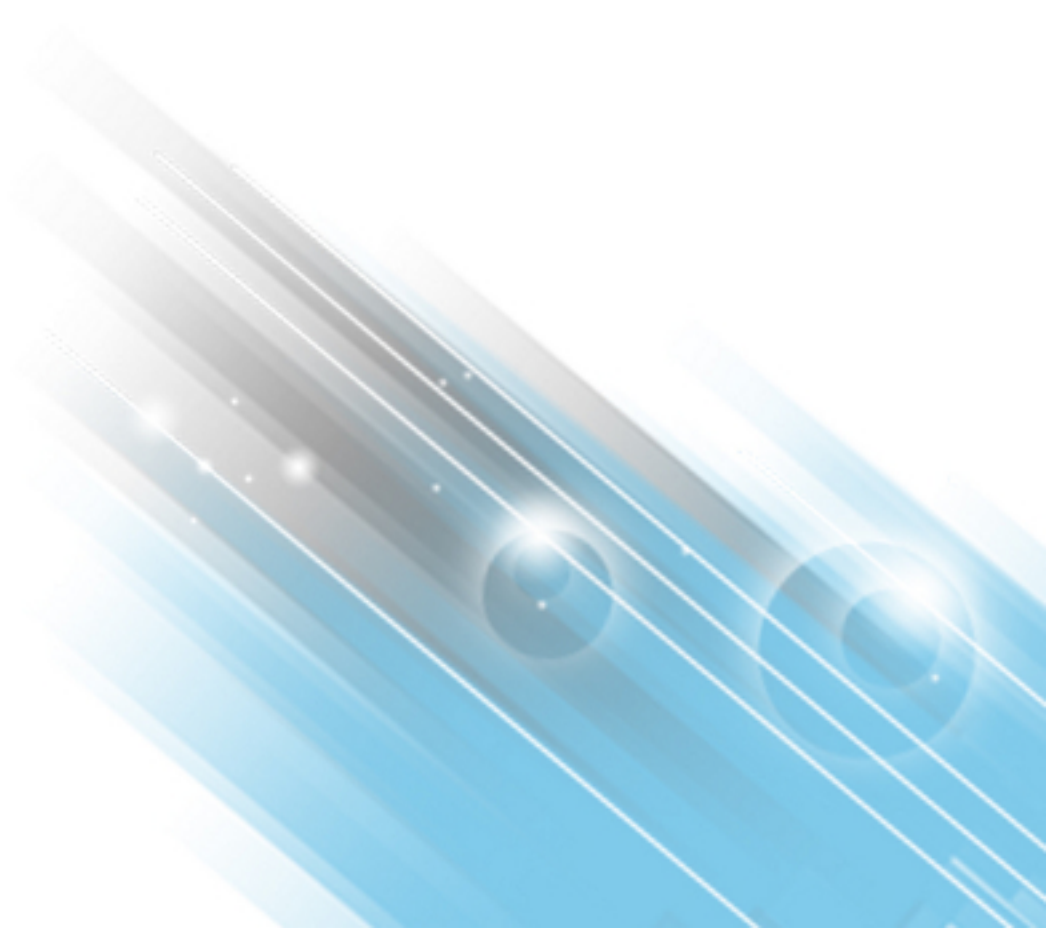


HP ArcSight ESM Express

Software Version: 6.9.0c

Installation Guide

August 24, 2015



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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

Copyright Notice

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

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

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

Support

Contact Information

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

Contents

Chapter 1: What Is ESM With CORR-Engine Storage?	7
ESM Express Components	7
ArcSight Manager	7
CORR-Engine	8
ArcSight Command Center	8
ArcSight Console	8
SmartConnectors	8
Deployment Overview	8
ESM Express Communication Overview	9
Effect on Communication When Components Fail	9
Choosing between FIPS Mode or Default Mode	10
Mode Comparison	10
Using PKCS #11	11
Import Control Issues	11
Directory Structure for ESM Installation	12
References to ARCSIGHT_HOME	12
Chapter 2: Installing ESM Express	13
Starting the ESM Express Appliance for the First Time	13
Using the Configuration Wizard	14
Rerunning the ESM Configuration Wizard	17
Chapter 3: Post-Installation Considerations	19
Setting Up ESM Reports to Display in a Non-English Environment	19
On the Manager	19
On the Console	19
The Next Steps	20
Chapter 4: Installing ArcSight Console	22
Console Supported Platforms	22
Required Libraries for RHEL and CentOS (64 Bit)	22
Installing the Console	23
Configuring the ArcSight Console	24

Importing the Console's Certificate into the Browser	29
Character Set Encoding	29
Starting the ArcSight Console	30
Logging into the Console	31
Reconnecting to the ArcSight Manager	32
Reconfiguring the ArcSight Console	32
Uninstalling the ArcSight Console	32
Appendix A: Troubleshooting	34
Location of Log Files for Components	34
Customizing the Manager	36
Fatal Error when Running the First Boot Wizard	36
Changing the Host Name of the Machine after Running the First Boot Wizard	37
Appendix B: Default Settings For Components	39
General Settings	39
CORR-Engine Settings	39
Manager Settings	39
Appendix C: Using PKCS	41
PKCS#11	41
PKCS#11 Token Support in ESM Express	41
PKCS#12	42
Setting Up to Use a PKCS#11 Provider	42
Install the PKCS#11 Provider's Software	43
Map a User's External ID to the Subject CN	43
Obtain the CAC/90Meter's Issuers' Certificate	45
Extract the Root CA Certificate From the CAC/90Meter Certificate	47
Import the CAC/90Meter Root CA Certificate into the ArcSight Manager	49
FIPS Mode - Import into the ArcSight Manager's nssdb	49
Default Mode - Import into ArcSight Manager's Truststore	50
Select Authentication Option in ArcSight Console Setup	51
Logging in to the ArcSight Console Using PKCS#11 Token	52
Logging in to an ESM Web UI Using PKCS#11 Token	53
Appendix D: Installing ESM in FIPS Mode	55

What is FIPS?	55
Network Security Services Database (NSS DB)	55
What is Suite B?	56
NSS Tools Used to Configure Components in FIPS Mode	57
TLS Configuration in a Nutshell	57
Understanding Server Side Authentication	58
Understanding Client Side Authentication	58
Exporting the Manager's Certificate to Clients	58
Using PKCS #11 Token With a FIPS Mode Setup	59
Installing ArcSight Console in FIPS Mode	59
Types of Key Pairs Used in FIPS Mode	61
Connecting a Default Mode ArcSight Console to a FIPS 140-2 ArcSight Manager	62
Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers	63
Configure Your Browser for FIPS	63
Installing SmartConnectors in FIPS Mode	63
How do I Know if My Installation is FIPS Enabled?	65
Appendix E: Locales and Encodings	66
Terminology	66
Character Set	66
Code Point	66
Code Set	66
Encoding	66
Internationalization	66
Locale	67
Localization	67
Unicode	67
UTF-8	67
Before you Install a Localized Version of ArcSight ESM	67
ArcSight Console and Manager	67
ArcSight SmartConnectors	68
Setting the Encoding for Selected SmartConnectors	68
Localizing Date Formats in Tokens and Operations	68
agent.parser.locale.name Values	68
Key-Value Parsers for Localized Devices	74

Appendix F: Restore Appliance Factory Settings 75

Send Documentation Feedback76

Chapter 1: What Is ESM With CORR-Engine Storage?

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

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

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

ESM Express is ESM on an HP-supplied appliance, but with a different licensing model and feature set than software ESM.

ESM Express Components

The ESM Express system comprises the following components:

- ["ArcSight Manager" below](#)
- ["CORR-Engine" on the next page](#) (Correlation Optimized Retention and Retrieval Engine)
- ["ArcSight Command Center" on the next page](#)
- ["ArcSight Console" on the next page](#)
- ["SmartConnectors" on the next page](#)

ArcSight Manager

The ArcSight Manager is at the center of the ESM Express system. The Manager is a software component that functions as a server that receives event data from Connectors and correlates and stores them in the database. The Manager also provides advanced correlation and reporting capabilities. The Manager and CORR-Engine are integrated components and get installed on the same machine.

CORR-Engine

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

ArcSight Command Center

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

- Enables you to perform many of the functions found in the ArcSight Console.
- Provides dashboards, a variety of search types, reports, case management, notifications, channels, and administrative functions for managing content, users, connectors, storage, archives, search filters, saved searches, and peer configuration.

ArcSight Console

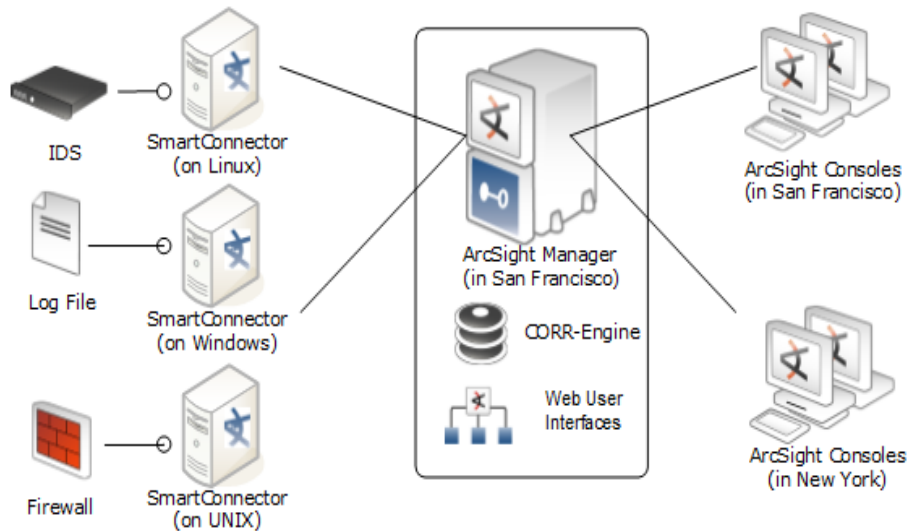
The ArcSight Console provides a user interface for you to perform administrative tasks, such as fine tuning the ESM content, creating rules, and managing users. The ArcSight Console is installed separately on client machines.

SmartConnectors

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

Deployment Overview

The following is an example of how various ESM components can be deployed in a network.



0

ESM Express Communication Overview

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

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

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

Effect on Communication When Components Fail

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

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

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

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

If a SmartConnector fails, whether event data loss will occur or not depends on the SmartConnector type. SmartConnectors that listen for events from devices such as the SNMP SmartConnectors will

stop accepting events. However, a SmartConnector that polls a device, such as the NT Collector SmartConnector, may be able to collect events that were generated while the SmartConnector was down, after the SmartConnector comes back up.

Choosing between FIPS Mode or Default Mode

ESM Express supports the Federal Information Processing Standard (FIPS) 140-2 and Suite B. FIPS 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 FIPS 140-2 standards.

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

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

Mode Comparison

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

Mode	Use of SSL/TLS	Default Cipher Suites	Keystore/Truststore
Default Mode	SSL	<ul style="list-style-type: none">• TLS_RSA_WITH_AES_128_CBC_SHA• SSL_RSA_WITH_3DES_EDE_CBC_SHA• More...	Keypair and Certificates stored in Keystore and cacerts, and Truststore in JKS format
FIPS 140-2 Mode	TLS	<ul style="list-style-type: none">• TLS_RSA_WITH_AES_128_CBC_SHA• SSL_RSA_WITH_3DES_EDE_CBC_SHA	Keypair and Certificates stored in NSSDB

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

Using PKCS #11

ArcSightESM Express supports the use of a PKCS#11 token such as 90Meter or the Common Access Card (CAC) (which is used for identity verification and access control) to log into the Console. 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.”

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

Import Control Issues

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

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

This is appropriate for most countries. However, if your government mandates restrictions, back up 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
```

Rename *.jar.original to *.jar.

The only impact of using the restricted version files would be that you cannot import unrestricted-strength key pairs. Also, you cannot save the keystore if you use passwords that are longer than four characters. No other ESM Express functionality is impacted.

Directory Structure for ESM Installation

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

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

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

References to ARCSIGHT_HOME

`<ARCSIGHT_HOME>` in the paths represents:

- `/opt/arcsight/manager` for the ArcSight Manager
- Whatever path you specified when you installed the ArcSight Console
- Whatever path you specified when you installed an ArcSight SmartConnector.

Chapter 2: Installing ESM Express

Read the Release Notes before you begin installing ESM Express.

There are no preparations necessary on the appliance and no opportunity to make any preparatory adjustments before the First Boot Wizard starts. However, it is essential that a network cable be plugged in to eno1 (the left-most cable slot). The Operating System First Boot Wizard initializes only eno1, and if the network cable is plugged in to a different slot, the Manager does not have a network connection, unless you manually configure that slot.

Starting the ESM Express Appliance for the First Time

When you power on the ESM Express appliance, the Operating System First Boot Wizard (FBW) starts automatically.

This is a command line interface. The FBW asks you to supply the following information, one entry at a time (the FBW indicates which values are optional):

1. At appliance login, log in as user *root*, using the password *arcsight*.
2. Set a new password for user *root*.
3. Set a new password for user *arcsight*.
4. Set the appliance hostname.
5. Specify the IP address (IPv4 only). You might need to get this and the following values from your system administrator.
6. Specify the netmask.
7. Specify the default gateway.
8. Specify the primary DNS IP Address (IPv4 only)
9. Specify the secondary DNS IP Address (IPv4 only)
10. Specify the DNS Search Domains.
11. Specify the time zone. You can start to type and press Tab and the system will attempt to auto-fill the time zone. For example you can type A, Tab and it fills in "America_". Press the Tab key twice for a list of timezone entries that starts with "America_".
12. Enter the Date. (The date and time are optional if you specify an NTP server.)

13. Enter the Time.
14. Specify the NTP servers. List one NTP server per line.

When you are done, it provides a list of what you have specified, for you to review. If you say No, it starts over.

If you accept the specifications then press **Enter** to end the installation session and start the Configuration Wizard.

Although the installer session provides a command for starting the Configuration Wizard manually, do not use it. The Configuration Wizard starts automatically when you press **Enter** to end the installer session.

Using the Configuration Wizard

When installing ESM Express, the configuration wizard starts automatically.

1. Read the Welcome message. If the license file is accessible, type **yes** to continue.
2. Under **Language Options**, select the language for interface displays. Press **Enter** to continue.
3. Under **CORR-Engine Password**, press **Enter** to continue with obfuscated passwords or type **no** and **Enter** to allow them to show on screen.
4. Under **CORR-Engine Password**, set a password for the CORR-Engine and reenter it in the Password confirmation text box and press **Enter**. For information on password restrictions, see the Administrator's Guide for ESM Express, chapter "Configuration", section "Managing Password Configuration".
5. Under **CORR-Engine Configuration**, enter the CORR-Engine storage allocation information and press **Enter**.

System Storage Size - the size of the storage space set aside to store resources

Event Storage Size - the size of the storage space set aside to store events

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

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

6. Under **Notification Emails**, specify the following email addresses:

Error Notification Recipients: Specify one email address for the email account to receive email notifications if the Manager goes down or encounters some other problem.

From email address: The email address used for the notifications sender.

If the values are correct, type **yes** and **Enter** to continue.

7. On the **License File** panel, enter the path and file name of the license file you downloaded and press **Enter**.
8. Under **Select the Product Mode**, select whether you want to install in default mode or FIPS mode. Press **Enter** to continue.

Caution:

- If you choose to install the product in FIPS mode, be sure to install the Console in FIPS mode too. Refer to ["Installing ArcSight Console in FIPS Mode" on page 59](#) for instructions on installing the Console in FIPS mode.
- Once you have configured the software in FIPS mode, you will not be able to convert it to default mode without reinstalling it.
- Converting from default mode installation to FIPS mode is supported. If you need to do so at any time, refer to the Administrator's Guide for instructions.
- By default, ESM 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 configuration wizard completes successfully. Refer to the Administrator's Guide for ESM Express for details on using a CA-signed certificate.

9. If you selected FIPS mode, confirm your selection. If not, skip to the Manager Information step.
10. If you selected FIPS mode on the **Select the Cipher Suite Options** panel, 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 means more security, it also means computational cost in time and resource (CPU) consumption. In most scenarios, the 128-bit key size is sufficient.

11. Under **Manager Information**, enter the Manager's hostname or IP address, set the user ID and password for the admin user, and press **Enter**.

Caution: Manager host name is the local host name, IP address, or fully-qualified domain

name of the machine where the Manager is installed. This name is what all clients (for example, ArcSight Console) specify to connect to the Manager. Using a host name and especially a fully-qualified domain name instead of an IP address is recommended for flexibility.

If you do not want the hostname on your DNS server, add a static host entry to the `/etc/hosts` file to resolve the hostname locally.

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

Although the Manager uses a self-signed certificate by default, you can switch to using a CA-signed certificate if needed. You can do this after installation. Refer to the Administrator's Guide for instructions.

12. Under **Packages**, ESM Express does not license these packages. Press **Enter** to continue. There are default standard content packages that are installed automatically on the ArcSight Manager. These default packages provide essential system health and status operations, and you can use them immediately to monitor and protect your network.

For more information about packages, see the *ArcSight Administration and ArcSight System Standard Content Guide*.

13. Under **About to Configure ESM**.

Caution: Once you type **yes** and press **Enter**, the product is installed as specified.

14. When the configuration says **Configuration Completed Successfully**, type **Yes** and then **Enter** to exit.
15. **Important!** This step is required in order to start the services. Log in as user `root` and run the following script to set up the required services:

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

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

You can rerun the wizard manually only if you exit it at any point **before** you reach the first configuration screen called "About to Configure ESM Express v6.9.0c". See ["Rerunning the ESM Configuration Wizard" on the next page](#) for details.

Rerunning the ESM Configuration Wizard

You can rerun the wizard manually only if you exit it at any point **before** the actual configuration begins. That section is entitled: "About to Configure ESM"

If for any reason you cancel out of the wizard or run into an error before the configuration begins, you can rerun the wizard manually.

1. To rerun the configuration wizard use the following command:

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

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

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

If you encounter a failure during the configuration stage, restore the appliance to its factory settings and start over. See ["Restore Appliance Factory Settings" on page 75](#).

Chapter 3: Post-Installation Considerations

This section includes information about rerunning the installation and configuration wizard.

Setting Up ESM Reports to Display in a Non-English Environment

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

On the Manager

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

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

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

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

Add the following line:

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

Save the file.

3. Restart the Manager by running:

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

4. In the ArcSight Console, select the Arial Unicode MS font in all the report elements, including the report template. This is described in the next topic.

On the Console

Set preferences in the Console and on the Console host machine.

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

On Windows: Edit `console.bat`

On 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

4. Set the font preferences for your reports, as described in, "Using Report Templates" in the ArcSight Console User's Guide.

The Next Steps

- **Install ArcSight Console**

Download the ArcSight Console and install it on a supported platform. Refer to the chapter on installing the Console, for details on how to do this. For performance reasons, install the ArcSight Console on a different machine than your ESM installation.

- **Access ArcSight Command Center**

Refer to the *ArcSight Command Center User's Guide* for more information on using the ArcSight Command Center.

- **Read the Release Notes**

The release notes for this release are available on [Protect 724](#).

- **Download Use Cases**

To get up and running quickly, HP ArcSight now offers Security Use Case packages available for download at <https://arcsight.hpwsportal.com/catalog.html#/Home/Show>. These packages provide essential security monitoring for network systems (such as IDS/IPS, VPN, Firewall), and packages that monitor and analyze the event stream for critical security concerns, such as anomalous traffic and suspicious outbound traffic.

- **Changing the Manager Heap Size**

The default Manager heap size is 8 GB. To improve the ESM Manager's performance, change the heap size to 16 GB. To change the Manager's heap size after the installation completes, refer to the *ArcSight Command Center User's Guide*.

Chapter 4: Installing ArcSight Console

The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of the ArcSight Command Center) to ArcSight ESM Express. This chapter explains how to install and configure the ArcSight Console in default mode. To install the Console in FIPS mode, see ["Installing ArcSight Console in FIPS Mode" on page 59](#). Section ["Choosing between FIPS Mode or Default Mode" on page 10](#) lists the basic differences between the modes.

Make sure the Manager is running before installing the ArcSight Console. Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager.

Console Supported Platforms

Refer to the *HP ArcSight ESM Support Matrix* document available on the Protect 724 site for the most current information on supported platforms and browsers.

Required Libraries for RHEL and CentOS (64 Bit)

On the RHEL and CentOS 6.x and later 64-bit workstations, the Console requires the latest versions of following libraries:

```
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
libXrender-0.9.7-2.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
```

Installing the Console

The notes that follow include important considerations for Installing the ArcSight Console on different operation systems.

Note: Linux:

Do not attempt to install the Console as the root user on Linux-based machines. If you do, the installer prompts you to change ownership of certain directories after the installation completes, so we recommend you perform all of the following steps as a non-root user. This issue does not apply to Windows machines.

Note: On Macintosh platforms, please make sure that:

- You are using an Intel processor based system.
- Keep in mind that keytoolgui does not work on the Mac, so use keytool commands, documented in the *ESM Administrator's Guide*, whenever you need to manage the keystore or certificates.
- Before you start the Console, make sure to set up a default printer to which to print. if you open a channel, select some rows, right-click on them and select **Print Selected Rows** from the resulting menu, the Console will crash if a default printer is not set up.

Make sure that ArcSightESM is installed before installing the ArcSight Console.

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

Platform	Installation File
Linux	ArcSight-6.9.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-6.9.x.nnnn.y-Console-Win.exe
Macintosh	ArcSight-6.9.x.nnnn.y-Console-MacOSX.zip

The location of the installer's log files are shown below:

Platform	Installation Log Files
Linux	/home/<user>

Platform	Installation Log Files
Windows	C:\Users\ <user>< td=""></user><>
Macintosh	/Users/<user>

2. Click **Next** in the **Installation Process Check** screen.
3. Read the introductory text in the **Introduction** panel and click **Next**.
4. On the **License Agreement** panel, the “I accept the terms of the License Agreement” radio button is disabled until you 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**.
5. Read the text in the **Special Notice** panel and click **Next**.
6. On the **Choose ArcSight installation directory** panel, you can accept the default installation directory, click **Choose** to navigate to an existing folder, or type in a path to where you want to install the Console. If you specify a folder that does not exist, the folder is created for you.

Caution: Do not use spaces in install paths. This includes Linux, Macintosh, and Windows systems. The Console installer does not display any error message, but the Console will not start.

7. On the **Choose Shortcut Folder** panel, select where you would like to create a shortcut for the Console and uninstall icons and click **Next**.
8. 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.

Note: On Windows, when the installer is configuring the Console (the **Please Wait** panel), you might see a message that the TZData update was not successful. If you get that message, click OK and continue. The Console installs successfully. Usually, TZData is correctly updated regardless of this message. To make sure check that the time stamp on the files in the C:\arcsight\Console\current\jre\lib\zi.tzdata_2014j_1\ directory matches the date and time when you installed the Console. If the time stamp is old or the files are missing, uninstall then re-install the Console.

Configuring the ArcSight Console

After the Console has been installed, you will need to configure it.

1. 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**.
2. Select the mode in which you would like to configure the Console, Default or FIPS.

Select the same mode in which the Manager is installed.

If you select **Run console in FIPS mode**, you get a warning that once you switch to FIPS mode you cannot revert to default mode and are asked if you want to continue.

(FIPS mode only) You will be prompted to select a cipher suite. The choices are:

- FIPS 140-2
- FIPS with Suite B 128 bits
- FIPS with Suite B 192 bits.

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**.

3. Enter the host name of the Manager to which the Console will connect.

Caution: Do not change the Manager's port number.

Click **Next**.

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

If you select the Use proxy server option, you will be prompted to enter the proxy server information **Proxy Host Name** and **Proxy Host**.

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

5. The ArcSight Console configuration wizard prompts you to choose the type of client authentication you want to use. The choices are:
 - Password Based Authentication
 - Password Based and SSL Client Based Authentication

- Password Based or SSL Client Based Authentication
- SSL Client Only Authentication

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

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

If you select **Password Based Authentication**, you to log in with a user name and password.

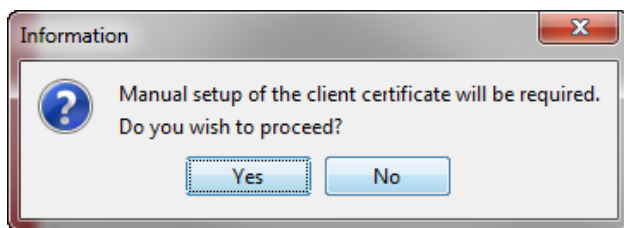
If you select **Password Based and SSL Client Based Authentication**, you need a client certificate to log in, in addition to your user name and password. Follow the procedure described in ESM Administrator's Guide to set up the client certificate.

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

- Client Key Store
- PKCS#11 Token

If you plan to use a PKCS #11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the Console, you can refer to "[Setting Up to Use a PKCS#11 Provider](#)" on page 42 for instructions on how to set up the token.

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



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

6. 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.

Browse to and select the **Browser Executable** and click **Next**.

7. Select whether this installation of the Console will be used by a single user or multiple users.

You can choose from these options:

- This is a single system user installation. (Recommended)

Select this option when:

- There is only one system account on this machine that one or more Console users will use to connect to the Console. For example, a system account, admin, is used by Console users Joe, Jack, Jill, and Jane.

OR

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

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

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

- Multiple users will use this installation

Select this option when:

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

AND

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

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

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

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

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

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

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

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

On Windows, when the installer is configuring the Console (the **Please Wait** panel), you might see a message that the TZData update was not successful. If you get that message, click OK and continue. The Console installs successfully. Usually, TZData is correctly updated regardless of this message. To make sure check that the time stamp on the files in the `C:\arcsight\Console\current\jre\lib\zi.tzdata_2014j_1\` directory matches the date and time when you installed the Console. If the time stamp is old or the files are missing, uninstall then re-install the Console.

8. You have completed configuring your ArcSight Console. Click **Finish** on the final panel to close the configuration wizard.
9. Click **Done** in the next screen.
10. For best results, install the ArcSight Console on an operating system that is set to the same locale as the Manager. During startup, the ArcSight Console and the Manager automatically detect and use the locale from the operating system.

However, if you are installing the Console on a Linux machine, edit the file `/home/arcsight/.bash_profile` by adding the line:

```
export LANG=[language].UTF-8
```

...where `[language]` is one of these:

`en_US` (English)

`zh_CN` (Simplified Chinese)

zh_TW (Traditional Chinese)
ja_JP (Japanese)
fr_FR (French)
ko_KR (Korean)
ru_RU (Russian)

Importing the Console's Certificate into the Browser

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

1. Export the keypair from the Console. For more information, refer to the *ESM Administrator's Guide* in the "Export a Key Pair" topic.
2. Import the Console's keypair into the browser.

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

Character Set Encoding

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

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

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

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

If you must use a non-UTF-8 encoding, and you must have user IDs with other characters in them, custom shortcut keys are not supported on any Console where these users would log in. In that situation, add the following property to the console.properties file:

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

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

Starting the ArcSight Console

Note: On the ArcSight Console machine, for any special IPv4/IPv6 configurations that do not match the DNS server entries, you can instruct the ArcSight Console how to connect to ESM by providing an additional option, `java.net.preferIPv6Addresses`. Do that by setting the environment variable `ARCSIGHT_JVM_NET_OPTIONS`.

For example, to instruct an ArcSight Console using IPv6 DNS entries, use the following commands:

On Unix

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

On Windows

```
set ARCSIGHT_JVM_NET_OPTIONS=-Djava.net.preferIPv6Addresses=true
```

After installation and setup is complete, start ArcSight Console using the shortcuts installed or open a command window on the Console’s `bin` directory and run:

On Windows:

```
arcsight console
```

On Unix:

```
./arcsight console
```

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

If you selected...	You will see the following buttons...
Password Based Authentication	Login Cancel
Password Based and SSL Client Based Authentication	Login Cancel

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

Note: Under certain circumstances, you might see a Login Failed message that, for the cacerts folder, access is denied. Ensure that the *arcsight* user has write access to the cacerts file. If this does not clear the problem, and you are on a Windows system, the cause may be due to file locks on the cacerts file. These may be cleared by rebooting your computer.

Logging into the Console

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

To start the Console, click **Login**. When you start the Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the Manager's certificate. The prompt will

show details specific to your settings. Click **OK** to trust the Manager's certificate. The certificate will be permanently stored in the Console's truststore and you will not see the prompt again the next time you log in.

Reconnecting to the ArcSight Manager

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

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

Reconfiguring the ArcSight Console

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

On Windows: `arcsight.bat consolesetup`

On Linux: `./arcsight consolesetup`

and follow the prompts.

Uninstalling the ArcSight Console

Before uninstalling the ArcSight Console, exit the current session.

To uninstall on Windows, run the **Start > All Programs > ArcSight ESM 6.9c Console > Uninstall ArcSight ESM Console 6.9c** program. If a shortcut to the Console was not installed on the Start menu, locate the Console's UninstallerData folder and run:

`ArcSight_ESM_Console_6.9c.exe`

To uninstall on Unix hosts, run the uninstaller program from either the directory where you created the links while installing the product or if you had opted not to create links, then run this from the `/opt/arcsight/console/current/UninstallerData` directory:

`./ArcSight_ESM_Console_6.9c`

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

`./Uninstall_ArcSight_ESM_Console_6.9c`

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

Appendix A: Troubleshooting

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

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

Location of Log Files for Components

The log files can be found in the following location:

Log file name	location	Description
First Boot Wizard Logs		
fbwizard.log	/opt/arcsight/manager/logs/default/	Contains detailed troubleshooting information logged during the steps in "Using the Configuration Wizard" on page 14.
firstbootsetup.log	/opt/arcsight/manager/logs/	Contains brief troubleshooting information about commands that ran during the steps in "Using the Configuration Wizard" on page 14.
CORR-Engine Log Files		
logger_server.log	/opt/arcsight/logger/current/arcsight/logger/logs	Contains troubleshooting information about the CORR-Engine

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

Log file name	location	Description
monit.log	/opt/arcsight/services/monit/data/	Contains timing information from startup and shutdown of ArcSight service processes.

Customizing the Manager

The First Boot Wizard allows you to configure the Manager and the CORR-Engine Storage. To customize a component further, you can follow these instructions to start the setup program for the component:

While logged in as user *arcsight*,

1. Stop the Manager if it is running:

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

2. Run the following command from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

3. Follow the prompts on the wizard screens. See the Administrator's Guide for information on any specific screen.

4. Restart the Manager after the wizard completes by running:

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

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 34](#).

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. You can rerun the First Boot Wizard if it did not reach the point where it configures the Manager. See section ["Rerunning the ESM Configuration Wizard" on page 17](#) for more details on this. If your error occurred before any component got configured, log in as user *root* and do the following:

Clear out (delete) the contents of the `/opt/arcsight` directory.

Rerun the setup using the following commands:

```
cd
/home/arcsight/install.esm/ESMComponents/service/opt/arcsight/services/bin/scripts
(All one line.)

./esm_setup.sh
```

If the above steps do not work, for example, if the setup has already started to configure the Manager or if your installation is corrupted, then restore the factory settings. See ["Restore Appliance Factory Settings" on page 75](#).

Changing the Host Name of the Machine after Running the First Boot Wizard

Wherever you see "host name," you may assume it means "host name or IP address."

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

Note: Run the `managersetup` command when logged in as user *arcsight*.

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

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

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

2. Change the host name or IP address of your machine.
3. Reboot the machine.
4. As the user *arcsight*, stop the Manager by running:

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

5. As the user *arcsight*, run the Manager's setup program from the `/opt/arcsight/manager/bin` directory as user *arcsight*:

```
./arcsight managersetup
```

- a. Enter the new host name or IP (that you changed 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 or IP.

If you are in FIPS mode, you do not get an option to regenerate a keypair. Manually delete the key pair, regenerate it, and go to the next step to restart the Manager.

6. As the user *arcsight*, start the Manager by running:

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

7. Start ArcSight Command Center by running:

```
https://<IP address>:8443/
```

Where **<IP address>** is the host name or IP address of the ESM Express. (Host names with underscores do not work on IE, so use the IP address.)

8. Import the Manager's certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the keytool. See the "Import a Certificate" topic in the "SSL Authentication" chapter in the *ESM Administrator's Guide*, available on the HP ArcSight Customer Support download site for details on how to do this.
9. Test to make sure that the clients can connect to the Manager.

Appendix B: Default Settings For Components

This appendix gives you the default settings for each software component in ESM.

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

General Settings

Setting	
default password for truststore	changeit
default password for cacerts	changeit
default password for keystore	password

CORR-Engine Settings

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

Setting	Default Value
Location of Logger	/opt/arcsight/logger
Database user name	arcsight
Database Port	3306

Manager Settings

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

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

Setting	Default Value
Location of Manager	/opt/arcsight/manager
Manager host name	Host name or IP address of ESM Express
Manager Port	8443
Manager Java Heap Memory	8 GB
Authentication Type	Password Based
Type of certificate used	Self-signed certificate
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"> 1. Stop the Manager by running the following command (as user <i>arcsight</i>): <code>/etc/init.d/arcsight_services stop manager</code> 2. Run the following command from the <code>/opt/arcsight/manager/bin</code> directory and set up the external SMTP server when prompted: <code>./arcsight managersetup</code> 3. Start the Manager by running (as user <i>arcsight</i>): <code>/etc/init.d/arcsight_services start manager</code>
Sensor Asset Auto Creation	true
Packages/default content installed	Default system content

Appendix C: Using PKCS

Public-Key Cryptography Standard (PKCS) comprises 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.

ArcSight ESM Express supports the use of a PKCS#11 token such as the Common Access Card (CAC) or 90Meter for identity verification and access control. It is used to log into the Manager from a user interface. 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 is running, in FIPS 140-2 mode or default mode.

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

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, Common Access Card (CAC), or 90Meter. The credentials of the authorized user are stored on the hardware itself. ESM 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#11 Token Support in ESM Express

ESM Express supports any PKCS#11 Token vendor that supports PKCS#11 2.0 or above. 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 ESM client is running (FIPS 140-2 mode or default mode). However, you must configure the ESM Manager to use “Password or SSL Authentication” when communicating with clients, which you set up by running the Manager Configuration Wizard, as documented in the chapter by that name in the Administrator Guide. It is easier to use the ArcSight Command Center, as follows:

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

To use a PKCS #11 token, make sure that the token's CA's root certificate and the certificate itself are imported into the ArcSight Manager's truststore. In the ArcSight Command Center, you can edit the External ID to match the common name on the Admin tab.

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

Setting Up to Use a PKCS#11 Provider

Even though ESM Express supports authentication through any PKCS#11 token, this appendix covers how to use the ActivClient's Common Access Card (CAC) as an example. The steps to set up a CAC card are:

1. ["Install the PKCS#11 Provider's Software" on the next page](#) on each client machine. That includes the ArcSight Console and every machine using a browser to access the ArcSight Command Center.
2. ["Map a User's External ID to the Subject CN" on the next page](#)
3. ["Obtain the CAC/90Meter's Issuers' Certificate" on page 45](#)
4. ["Extract the Root CA Certificate From the CAC/90Meter Certificate" on page 47](#)
5. ["Import the CAC/90Meter Root CA Certificate into the ArcSight Manager" on page 49](#)
6. ["Select Authentication Option in ArcSight Console Setup" on page 51](#)

Install the PKCS#11 Provider's Software

Before you use the PKCS#11 token, 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 a web-based interface. Refer to your PKCS#11 provider's documentation on how to install and configure it.

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

Install a proper PKCS#11 provider, such as 90Meter or ActivClient. Copying separate dlls might not be enough. In some cases a library specified in `arcsight_consolesetup` is just an entry point that needs other provider modules.

For ActivClient on 64-bit platforms always install both 32 and 64-bit components of ActivClient 6.2 or 7.0.2.

For 90Meter, install `SCM_1.2.25_64Bit_S.msi`. This comes with the 32-bit library as part of your install, which is required.

Map a User's External ID to the Subject CN

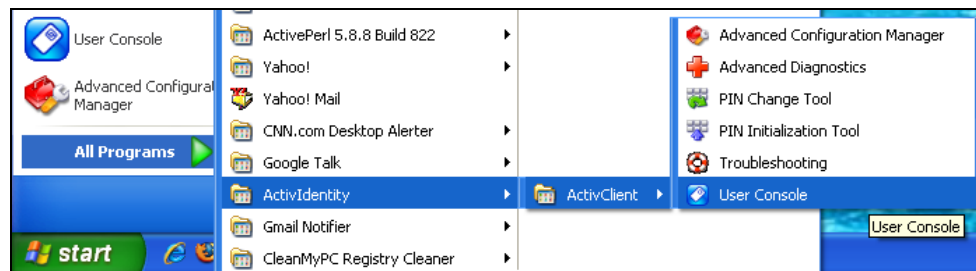
The CAC/90Meter card contains three types of certificate, Signature, Encryption, and ID certificates. The following instructions relate to identity certificate, which is used for SSL handshake during PKCS#11 login.

Map the Common Name (CN) on the PKCS#11 token 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 PKCS#11 token's ID certificate (include any spaces and periods that appear in the Common name). For example **john.smith.9691998563**. This allows the ArcSight Manager to know which user is represented by the identity stored in the PKCS#11 token.

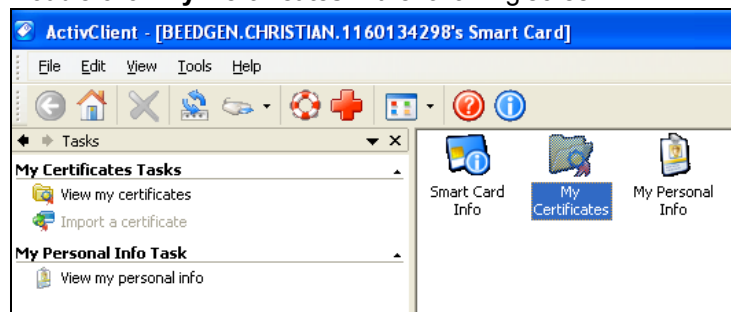
You can do this in the Command Center's **Admin** tab under User Management, when adding or editing a user.

The following screen shots demonstrate how to find the CN and map it to the User's External ID for ActivClient. It is just an example. For other PKCS#11 providers you would perform similar steps using different UI specific to the provider. Refer to the provider's documentation for instructions.

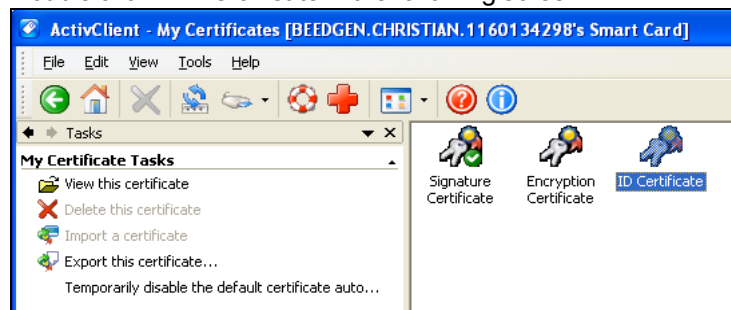
1. Obtain the Subject CN from the CAC/90Meter card.
 - a. Insert the CAC/90Meter card into the reader if not already inserted.
 - b. Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



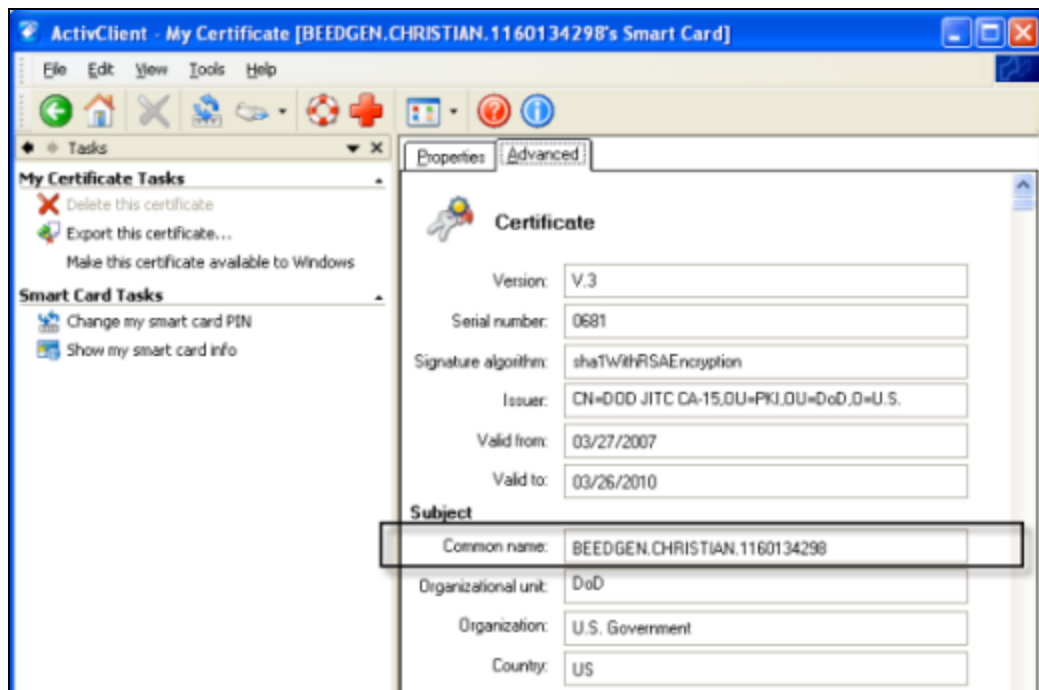
- c. Double-click **My Certificates** in the following screen:



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



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



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

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

- a. In the ArcSight Console, go to **Resources > Users > [user group]** and double-click the user whose External ID you want to map to the CAC/90Meter card common name. This opens 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/90Meter'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/90Meter device) is stored within the card itself. You need to export the CAC/90Meter'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:

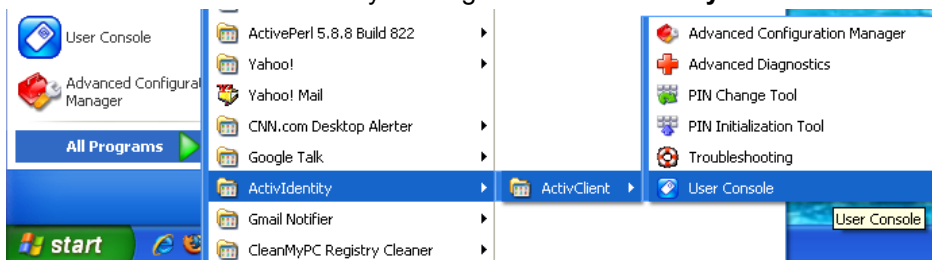
You can obtain the CAC/90Meter card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

Option 2:

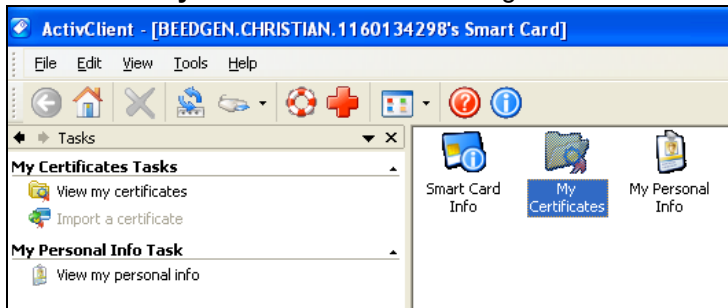
You can export the CAC/90Meter card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

The steps to extract the CAC/90Meter card's certificate from the card are:

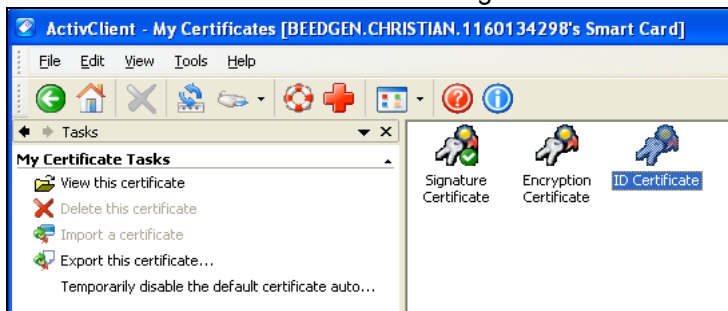
1. Insert the CAC/90Meter card into the reader if not already inserted.
2. Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



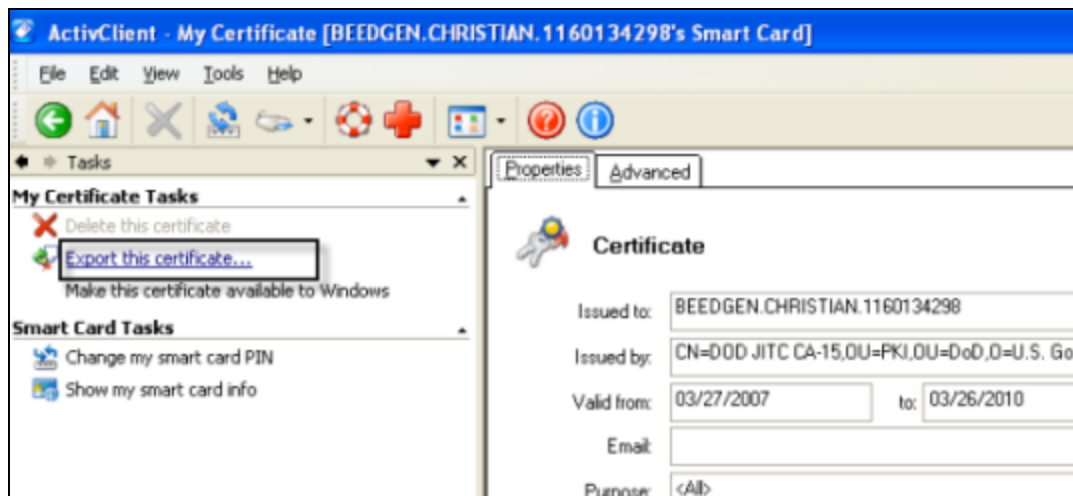
3. Double-click **My Certificates** in the following screen:



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



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



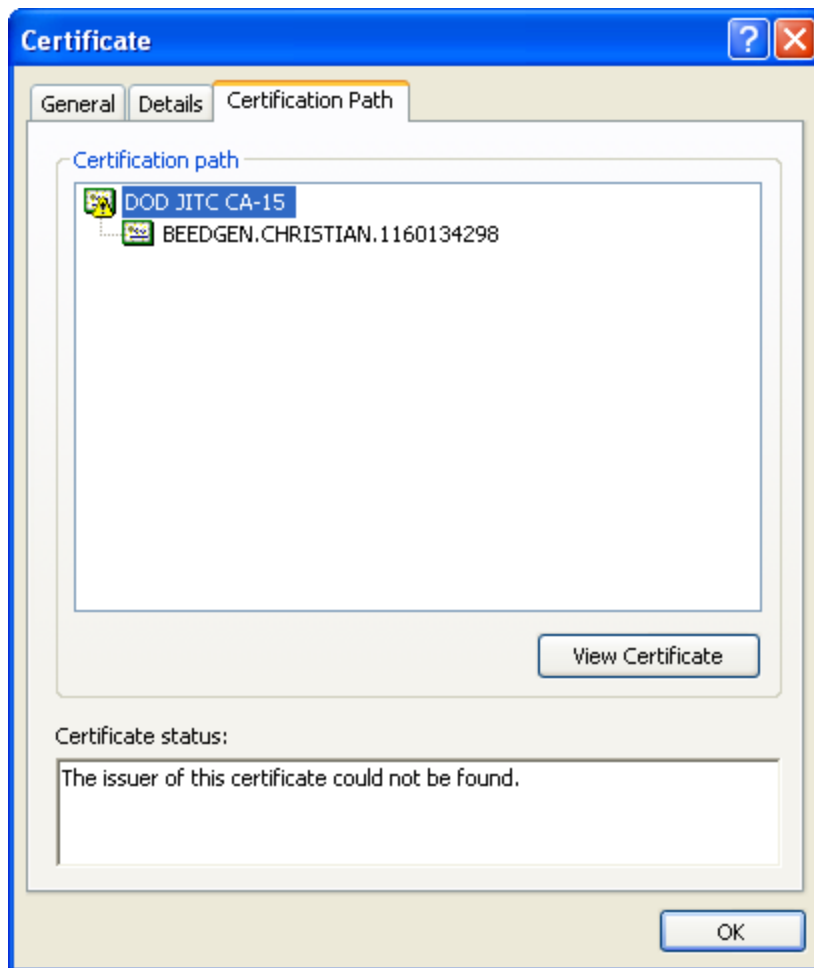
6. Enter a name for the certificate in the **File name** box and navigate to a location on your machine where you want to export it to and click **Save**.
7. When you see the success message, click OK.
8. Exit the ActivClient window.

Extract the Root CA Certificate From the CAC/90Meter Certificate

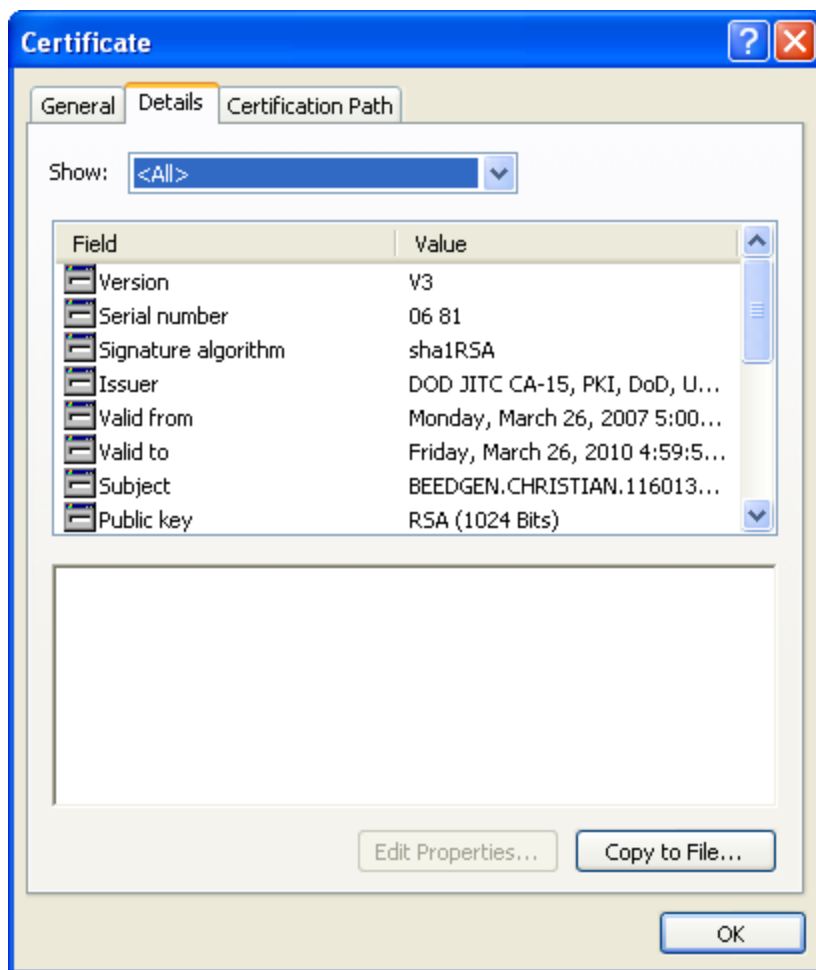
The CAC/90Meter certificate signer's CA root certificate and any intermediate signers' certificate(s) have to be imported into the ArcSight Manager's truststore.

Extract all intermediate certificates too (if any exist) using the following steps:

1. Double-click the certificate that you exported. The Certificate interface opens.
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/90Meter 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/90Meter certificate from which you extracted it.
7. Exit the Certificate dialog.

Import the CAC/90Meter 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. If the ArcSight Manager is running, log in as user *arcsight* and use this command:

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

2. Import the PKCS#11 token signer's CA root certificate by running:

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

Caution: 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:

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

Default Mode - Import into ArcSight Manager's Truststore

Use the following procedure to import the PKCS#11 token's root CA certificate into the ArcSight Manager's truststore.

If you do not have X Window installed, use the `keytool` command:

1. From <ARCSIGHT_HOME> launch `arcsight keytool -store managercerts -list` to see what's in ESM's trust store. There is no need to specify the exact location of ESM trust store, the tool uses ESM's config file to find it.
2. To remove certificate with alias *myKey*, run `arcsight keytool -store managercerts -delete -alias myKey`
3. To add a certificate and set an alias with spaces, such as JITC root CA 1 run:
`arcsight keytool -store managercerts -importcert -file /tmp/NSS-DoD-virtualJITC-SubCA1.cer -alias "JITC root CA 1"`
Do not miss the prompt: "Trust this certificate? [no]: yes" after the certificate key extensions are printed on the screen.

To get the list of keystore contents, run `arcsight keytool -store managercerts -list`.

If you have X Window installed, you may use `keytoolgui` instead of `keytool`:

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 directory

(/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*.
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. As user *arcsight*, restart the ArcSight Manager by running:

```
/etc/init.d/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 see the screen for the authentication option. The choices are:
 - Password Based Authentication
 - Password Based and SSL Client Based Authentication

- **Password Based or SSL Client Based Authentication**
 - **SSL Client Only Authentication**
4. Select the option for **Password or SSL Client Based Authentication**. You should also have chosen that option when you set up the ArcSight Manager.
 5. Follow the prompts in the next few screens by accepting the defaults.
 6. On the **Select client keystore type** screen select the **PKCS#11 Token** option.
 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 ActivClient, 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)

For 90Meter, always use the 32-bit library:

C:\Program Files\90meter\CACPIVMD\pkcs11\x86\LitPKCS11.dll

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

Logging in to the ArcSight Console Using PKCS#11 Token

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/90Meter card.)
- PKCS#11 Login

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

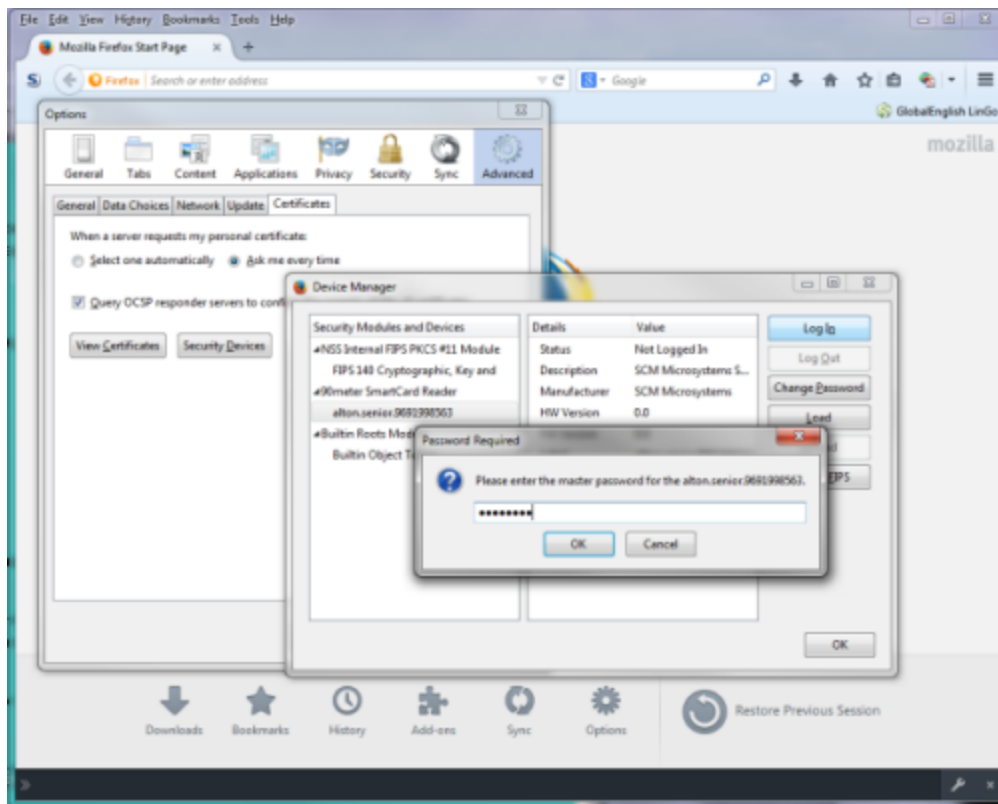
Logging in to an ESM Web UI Using PKCS#11 Token

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

1. Make sure that the PKCS#11 token is securely placed in its card reader.
2. Go to this web site: `https://<hostname>:8443/`.

If you are using Firefox, be sure to configure Firefox to work with ActivClient by loading the ActivClient module. For connections using a web browser you might need to configure the browser for some PKCS#11 providers:

- a. Open **Tools > Options** and go to the **Advanced > Certificates** tab.
- b. In **Security Devices** -select **Add a new module**.
- c. For "ActivIdentity" specify 32-bit dll by pointing to
C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll
For 90Meter everything is configured automatically.
- d. Use the **Log In** button to login to the module and enter the PIN when asked. Be sure to use the **Log Out** button to prevent auto-authentication.
- e. Restart Firefox and now you can log in to the ArcSight Command Center without any credentials.



3. You will be requested to enter your PIN.

If using Firefox, you see an exception. Click **Add exception**, then generate and confirm the certificate key. When you see the **User Identification Request** dialog. Click **OK**.

4. At the ArcSight Command Center login, *do not* enter any user ID or password. Leave them both blank and click **Login**. User authentication is resolved after you enter the PKCS#11 PIN in the dialog that appears next.
5. Enter your PIN in the Confirmation dialog. The dialog's title and appearance varies, depending on the PKCS#11 token configuration.

Appendix D: Installing ESM in FIPS Mode

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

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

If you are using FIPS mode, you cannot use the ArcSight Console on a Mac.

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.

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

Mozilla's Network Security Services (NSS) is an example of FIPS certified cryptographic module. It is the core and only cryptographic module used by ESM 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 ESM 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 \(NSS DB\)"](#) below, 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

Note: The default password for the NSS DB on every component is *changeit*. However, we recommend that you change this password by following the procedure in section “Changing the Password for NSS DB” in the ESM 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 to top secret information. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

Note:

- Not all ESM Express versions support the FIPS with Suite B mode. Refer to the ESM Express HP ArcSight ESM Support Matrix Document available on the Protect 724 website for supported platforms for FIPS with Suite B mode.
- When the Manager is installed in FIPS with Suite B compliant mode, all components (ArcSight Console, SmartConnectors, and Logger, if applicable) must be installed in FIPS with Suite B compliant mode, and browser used to access ESM Express must be FIPS enabled.
- Before installing ESM 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, ESM 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 unclassified up to secret information.

- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`

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

NSS Tools Used to Configure Components in FIPS Mode

NSS is a cross-platform cryptographic C library and a collection of security tools. ESM 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 ESM Express in FIPS mode, you need to set up TLS configuration on the ArcSight Manager, and ArcSight Console.

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 ESM 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 ArcSight Console. 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 ArcSight Console. 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 the section "Setting up Client-Side Authentication" in the Administrator's Guide.

Exporting the Manager's Certificate to Clients

This topic does not apply to ArcSight Console, which automatically imports the certificate. You are required to have this exported certificate available when installing clients that connect to this, such as Connectors. When installing the certificate, you import it into the clients' NSS DB. For Connectors, the

NSS DB is <ARCSIGHT_HOME>/current/user/agent/nssdb.client. Importing the ArcSight Manager's certificate allows the clients to trust the ArcSight Manager.

To export the 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.cer>
```

Note: 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.

Using PKCS #11 Token With a FIPS Mode Setup

To use a PKCS #11 Token, such as the ActivClient's Common Access Card (CAC) or 90Meter, follow the steps in "[Setting Up to Use a PKCS#11 Provider](#)" on page 42.

Installing ArcSight Console in FIPS Mode

Note: 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.

If you are using FIPS mode, you cannot use the ArcSight Console on a Mac.

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

Refer to the ESM 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**.
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 **Password Based or SSL Client Based Authentication**, which also must be 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. If you are using different authentication, you do not see this screen and you can skip this step.

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

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

On 64-bit Windows:

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

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

After completing the Configuration Wizard, follow the procedure in the topic “Setting up Client-Side Authentication,” in the “Configuration Changes Related to FIPS” appendix of the ESM Administrator’s Guide.

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.

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

Types of Key Pairs Used in FIPS Mode

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

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

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

1. Delete the existing Manager key pair.

If you are generating a key pair on the Manager, first delete the one that is there by default:

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

2. Generate a new key pair.

To generate a new key pair, you might use a command like this:

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

You can use `secp521r1`, but some browsers, such as Internet Explorer 11 (on Windows 8.1 and Windows Server 2012) and Chrome (on any operating system), cannot use the 521-bit option. The

examples in this document use 521, but if you are using IE 11 on those OS versions or Chrome, they *do not work* with FIPS Suite B. Use `secp384r1` (or `secp256r1`).

If you use the wrong elliptic curve cryptography for a browser that cannot support it, or you make a simple typographical error, there is no error or warning message and the Manager will not function correctly. To correct that problem delete Manager key pair and create it again.

3. Restart the Manager. Always restart the Manager after generating a key pair.
4. Delete the old Manager certificate from each client (connectors, ArcSight Console's, and browsers).
5. Export the new Manager certificate into each client. See ["Exporting the Manager's Certificate to Clients" on page 58](#). Leave the Connectors stopped. It may be preferable to deal with each connector one at a time, rather than turning them all off at once.
6. Restart the Console and the browser after importing the new Manager certificate.
7. In the ArcSight Console, delete each connector and then re-register it with the Manager.
8. Restart each connector.

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 an 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. See section, "Import a Certificate," in the *ESM Administrator's Guide*, for details on how to do this.

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 an ArcSight Manager's certificate into the ArcSight Console's `nssdb.client` manually, refer to the *ESM 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 the ArcSight Command Center.

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

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

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

When using a browser with Suite B, it matters how you generate your key pair. For information about the encryption to use with browsers, see ["Types of Key Pairs Used in FIPS Mode" on page 61](#).

Note: You cannot use IE or CHROME for 90Meter and CAC with FIPS Suite B (128 or 192) unless you set up your key pairs correctly.

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, (see the SmartConnector documentation) select **Enable FIPS Mode**. Then continue until you see the screen that offers you the choice to

Continue or Exit. Select **Exit** and click **Next**. On the next screen, click **Done**. 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 's certificate, run the following command from the connector's <ARCSIGHT_HOME>/current/bin directory:

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

Enter *changeit* for the password when prompted. That was the default password. If you changed it to something else, enter that password.

Run <ARCSIGHT_HOME>\current\bin\runagentsetup -i console to resume your connector setup. You can skip -i console to run this setup in GUI mode, but this documentation explains the procedure for running in console (command line) mode.

1. Select **Add a Connector** and press **Enter**.
2. Select the connector to configure and press **Enter** to continue.
3. For each of the parameters you are shown next, you can either change the value or accept the default value. Continue until you get to the Type of Destination parameters.
4. Select **ArcSight Manager (encrypted)** as the type of destination and press **Enter**.
5. Under **Destination Parameters**, or each of the parameters you are shown next, you can either change the value or accept the default value. When you get to them, enter the Manager Hostname and login credentials.
6. For the **FIPS Cipher Suites parameter**, choose from:
 - **FIPS Default**
 - **FIPS with Suite B128 bits**
 - **FIPS with Suite B192 bits**Press **Enter** to continue.
7. Enter the connector details such as the name and location, which can be any values you want.
8. Decide whether to install the connector as a service or leave it as a standalone application and press **Enter** to Continue.
9. Exit the connector configuration wizard.

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

How do I Know if My Installation is FIPS Enabled?

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

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

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 E: Locales and Encodings

ArcSight ESM supports various languages: English, Japanese, traditional Chinese, simplified Chinese, French, Russian, and Korean. 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 document describes the updates to be taken into consideration when configuring ArcSight ESM for a supported language.

Terminology

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

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 Point

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

Code Set

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

Encoding

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

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 region where you are running ArcSight ESM. A locale can include language, number format, date-time format, and other settings.

Localization

Localization is the process of adding language specific files to an internationalized application so that the application supports that language.

Unicode

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

UTF-8

The version of Unicode supported by ESM.

Before you Install a Localized Version of ArcSight ESM

Note: The ArcSight Manager and Console should be configured with the same locale.

By default, all communication between ArcSight components is done using UTF-8 character encoding. Even though ArcSight ESM 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 Manager.

ArcSight Console and Manager

For best results, install the ArcSight Console on an operating system that is set to the same locale as the Manager. During startup, the ArcSight Console and the Manager automatically detect and use 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

For some connectors you can set the encoding to a character set corresponding to your Locale. Check the SmartConnector Configuration Guide for that connector for instructions on configuring encodings. Such connectors support all character sets supported by Java.

Change the encoding to match the log files' encoding only if the log files use an encoding other than the default.

Connectors that do not specifically support an encoding specification use the default encoding of the operating system on which they reside.

Localizing Date Formats in Tokens and Operations

If your connector receives logs that contain timestamps or date formats in a non-English language or locale (for example, "mai 24, 2015 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 the `<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 in "[agent.parser.locale.name Values](#)" [below](#) for possible values for this property.

agent.parser.locale.name Values

The table below lists the possible values for this property.

Values	Language	Country	Variant
ar	Arabic		
ar_AE	Arabic	United Arab Emirates	
ar_BH	Arabic	Bahrain	

Values	Language	Country	Variant
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		

Values	Language	Country	Variant
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	
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	

Values	Language	Country	Variant
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		
fr_BE	French	Belgium	
fr_CA	French	Canada	
fr_CH	French	Switzerland	
fr_FR	French	France	

Values	Language	Country	Variant
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		

Values	Language	Country	Variant
nl_BE	Dutch	Belgium	
nl_NL	Dutch	Netherlands	
no	Norwegian		
no_NO	Norwegian	Norway	
no_NO_NY	Norwegian	Norway	Nynorsk
pl	Polish		
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	Slovenia	
sq	Albanian		
sq_AL	Albanian	Albania	
sv	Swedish		
sv_SE	Swedish	Sweden	
th	Thai		
th_TH	Thai	Thailand	

Values	Language	Country	Variant
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	

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=김

...where 김 is Korean for KIM.

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

If the received event message is:

우새르

...where 우새르 is Korean for User, then additional mapping is needed to translate 김 to User.

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

Appendix F: Restore Appliance Factory Settings

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

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

Use the following procedure to restore the appliance to its original, factory settings:

1. Attach a keyboard, monitor, and mouse directly to the appliance and open an operating system console session.
2. Reboot the appliance.
3. After a few minutes, when the Linux boot menu appears, use the down arrow key to select **System Restore <build_num>** from the menu that appears, then press **Enter**.

System Restore automatically detects and displays the archive image.

The image is named following this pattern:

YYYY-MM-DD_<model>_<build_num>.ari

where YYYY-MM-DD is the date, <model> is the appliance model, and <build_num> is the build number of the image being restored. If you encounter any issues with the image, contact Customer Support.

4. Press **F10** (VERIFY) to check the archive for damage before performing the restore.
5. Press **F1** (AUTOSELECT) to automatically map the source image.
6. Press **F2** (RESTORE) to begin the restore process.

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

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

Send Documentation Feedback

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

Feedback on Installation Guide (ESM Express 6.9.0c)

Just add your feedback to the email and click send.

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

We appreciate your feedback!