

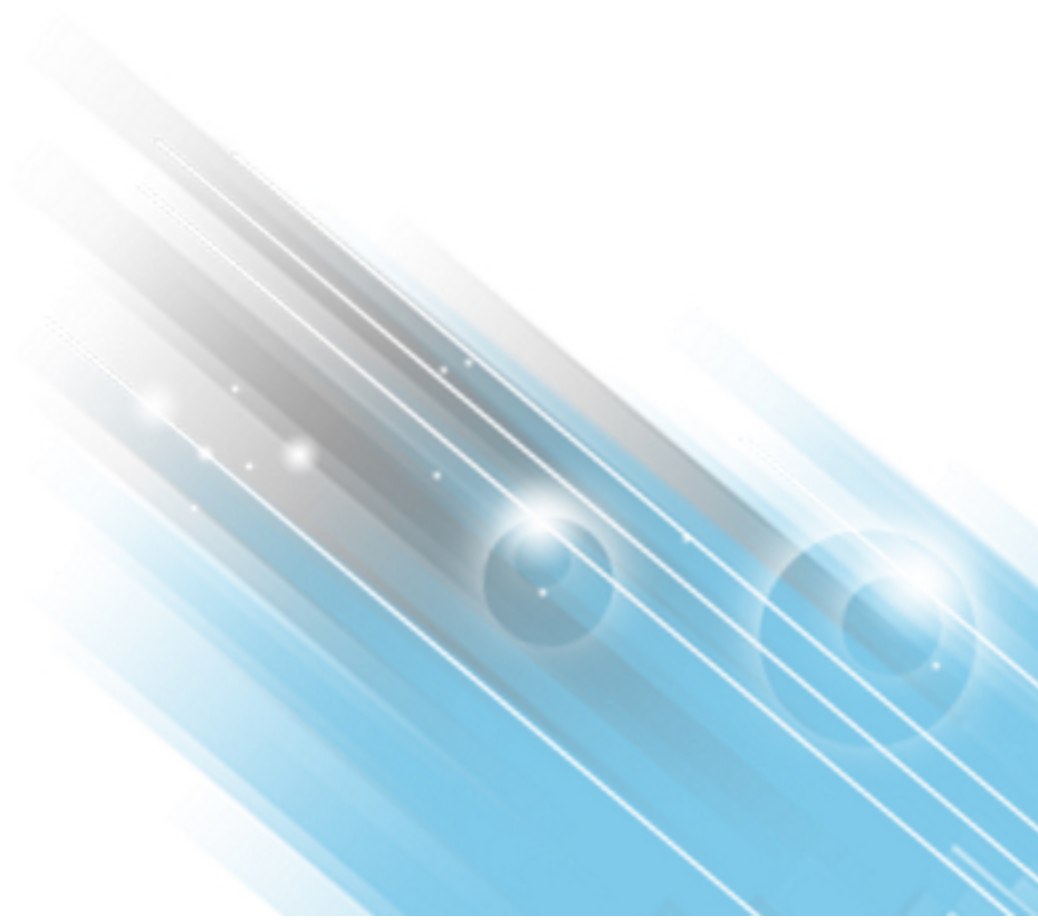


# HP ArcSight ESM

Software Version: 6.8c

## Installation and Configuration Guide

January 29, 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

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

# Contents

Chapter 1: What Is ESM With CORR-Engine Storage? .....	7
ESM Components .....	7
ArcSight Manager .....	7
CORR-Engine .....	8
ArcSight Command Center .....	8
ArcSight Console .....	8
SmartConnectors .....	8
ArcSight Web .....	8
Deployment Overview .....	9
ESM Communication Overview .....	9
Effect on Communication When Components Fail .....	9
Using PKCS #11 .....	10
Import Control Issues .....	10
Directory Structure for ESM Installation .....	11
References to ARCSIGHT_HOME .....	11
Securing Your ESM System .....	11
Protecting ArcSight Manager .....	11
ArcSightBuilt-In Security .....	13
Physical Security for the Hardware .....	13
Operating System Security .....	14
General Guidelines and Policies about Security .....	15
Chapter 2: Installing ESM .....	16
System Requirements .....	16
Supported Platforms .....	16
Before you Install ESM .....	17
Keep these TCP Ports Open .....	17
Install Time Zone Package .....	18
Preparing to Install .....	19
Set the /tmp Directory Size .....	19
Sizing Guidelines for CORR-Engine .....	19
Create User arcsight .....	21
Create /opt/arcsight Directory .....	22
Increase User Process Limit .....	22

Untar the tar File .....	23
Running the Installation File .....	23
Rerunning The Suite Installer .....	25
Running the Configuration Wizard In Console Mode .....	25
Configuring ESM .....	25
Handling a Time Zone Update Error .....	28
Changing the Manager Heap Size .....	28
Rerunning the ESM Configuration Wizard .....	29
Rerunning the ESM Configuration Wizard .....	29
Uninstalling ESM .....	29
Setting Up ESM Reports to Display in a Non-English Environment .....	30
On the Manager .....	30
On the Console .....	31
Improving the Performance of Your Server .....	32
The Next Steps .....	32
<b>Chapter 3: Installing ArcSight Console .....</b>	<b>33</b>
Console Supported Platforms .....	33
Required Libraries for RHEL and CentOS (64 Bit) .....	33
Using PKCS .....	34
Installing the Console .....	34
Configuring the ArcSight Console .....	36
Importing the Console's Certificate into the Browser .....	42
Character Set Encoding .....	43
Starting the ArcSight Console .....	43
Logging into the Console .....	45
Reconnecting to the ArcSight Manager .....	45
Reconfiguring the ArcSight Console .....	45
Uninstalling the ArcSight Console .....	45
<b>Appendix A: Troubleshooting .....</b>	<b>47</b>
Location of Log Files for Components .....	47
If You Encounter an Unsuccessful Installation .....	49
Customizing ESM Components Further .....	50
ArcSight Manager .....	50
ArcSight Web .....	50

Fatal Error when Running the First Boot Wizard .....	51
Changing the Hostname of Your Machine .....	51
Changing the Host Name of the Machine after Running the First Boot Wizard .....	53
<b>Appendix B: Default Settings For Components .....</b>	<b>56</b>
General Settings .....	56
CORR-Engine Settings .....	56
Manager Settings .....	56
ArcSight Web Settings .....	58
<b>Using PKCS .....</b>	<b>59</b>
PKCS#11 .....	59
PKCS#11 Token Support in ESM .....	59
PKCS#12 .....	60
Setting Up to Use a CAC Card .....	60
Install the CAC Provider's Software .....	60
Map a User's External ID to the CAC's Subject CN .....	61
Obtain the CAC's Issuers' Certificate .....	63
Extract the Root CA Certificate From the CAC Certificate .....	64
Import the CAC Root CA Certificate into the ArcSight Manager .....	66
Select Authentication Option in ArcSight Console Setup .....	67
Logging in to the ArcSight Console Using CAC .....	69
Logging in to ArcSight Command Center Using CAC .....	69
<b>Appendix C: Locales and Encodings .....</b>	<b>70</b>
Terminology .....	70
Character Set .....	70
Code Point .....	70
Code Set .....	70
Encoding .....	70
Internationalization .....	70
Locale .....	71
Localization .....	71
Unicode .....	71
UTF-8 .....	71
Before you Install a Localized Version of ArcSight ESM .....	71
ArcSight Console and Manager .....	71

- ArcSight SmartConnectors .....72
  - Setting the Encoding for Selected SmartConnectors .....72
  - Localizing Date Formats in Tokens and Operations .....72
  - agent.parser.locale.name Values .....72
  - Key-Value Parsers for Localized Devices .....78
- Send Documentation Feedback .....79

# 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 Components

The ESM 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 Web" on the next page](#)

## ArcSight Manager

The ArcSight Manager is at the center of the ESM 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 CenterESM 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 and ArcSight Web, which are still provided with ESM.
- 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 CORR-Engine. SmartConnectors are not bundled with ESM and are installed separately.

## ArcSight Web

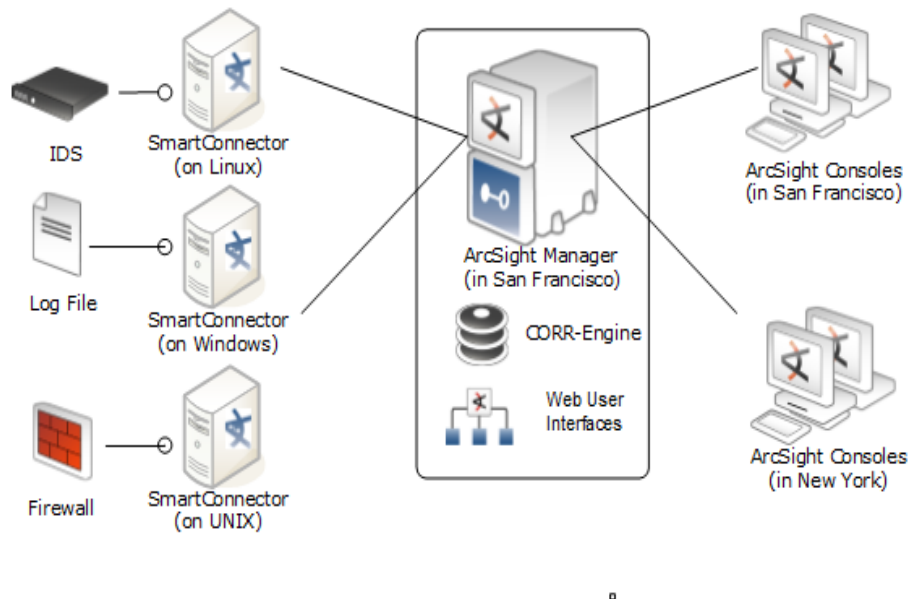
ArcSight Web is a web server that enables you to access the Manager securely using a browser.

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



## Deployment Overview

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



## ESM Communication Overview

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

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

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

## Effect on Communication When Components Fail

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

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

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

## Using PKCS #11

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

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 use ESM's keytoolgui to import unrestricted strength key pairs. Also, you cannot save the keystore if you use passwords that are longer than four characters. No other ESM functionality is impacted.

## Directory Structure for ESM Installation

By default, the ESM software 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/&lt;component&gt;/bin</code>
Properties files	<code>/opt/arcsight/&lt;component&gt;/config</code>
Log files	<code>/opt/arcsight/&lt;component&gt;/logs</code>

## References to ARCSIGHT\_HOME

`<ARCSIGHT_HOME>` in the paths represents:

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

## Securing Your ESM System

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

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

## Protecting ArcSight Manager

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

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

**Note:** <ARCSIGHT\_HOME> is the root directory for a component. For example for the Manager component, <ARCSIGHT\_HOME> is: /opt/arcsight/manager.

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

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

Port	Flow	Description
22/TCP	Inbound	SSH log in (Unix only)
53/UDP	Inbound/Outbound	DNS requests and responses
8443/TCP	Inbound	SmartConnectors and Consoles
25/TCP	Outbound	SMTP to mail server
110/TCP	Outbound	POP3 to mail server, if applicable
143/TCP	Outbound	IMAP to mail server, if applicable
1645/UDP	Inbound/Outbound	RADIUS, if applicable
1812/UDP	Inbound/Outbound	RADIUS, if applicable

Port	Flow	Description
389/TCP	Outbound	LDAP to LDAP server, if applicable
636/TCP	Outbound	LDAP over SSL to LDAP server, if applicable

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

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

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

```
web.accept.ips=192.0.2.0/24 192.0.2.5  
xmlrpc.accept.ips=192.0.2.0 192.0.2.5  
agents.accept.ips=10.*.*.*,192.0.2.0/255.255.0.0
```

## ArcSightBuilt-In Security

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

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

## Physical Security for the Hardware

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

Physical access to computers running ArcSight software must be restricted.

- Use the locking mechanisms provided by most rack-mount cases to prevent malicious/accidental tampering with the machine
- Use locks on disk drive enclosures

- Use redundant power and uninterruptible power supplies (UPS)
- Protect the BIOS (x86 systems only) or firmware:
  - Disable all CD-ROM drives for booting so that the system can only be booted from the hard disk
  - Disable COM, parallel, and USB ports so that they cannot be used to extract data
  - Disable power management

## Operating System Security

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

## General Guidelines and Policies about Security

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

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

Set up a login banner stating the legal policies for use of the system and the consequences of misuse. (Instructions for creating a login banner vary by platform.) ArcSight Consoles can also display a custom login banner. Contact the Customer Support using the HP SSO site for more information.

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

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

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

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

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

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

Use a firewall and intrusion detection systems to secure the network that the ArcSight Manager CORR\_Engine use.

## Chapter 2: Installing ESM

We recommend that you read the ESM Release Notes before you begin installing ESM.

If you are going to use the ESM High Availability Module with ESM and this is a new ESM installation, install the HA Module first. Refer to the ESM High Availability Module Guide for instructions.

**NOTE: ESM does not support FIPS in this release.**

## System Requirements

The hardware requirements for ESM 6.8c are as follows:

	Minimum	Mid-Range	High Performance
Processors	8 cores (16 preferred)	32 cores	40 cores
Memory	36 GB RAM (64 preferred)	64 GB RAM	1 TB RAM
Hard Disk	Six 600 GB disks (1.5 TB) (RAID 10)  15,000 RPM	20 1 TB disks (10 TB) (RAID 10)  10,000 RPM	12 TB (RAID 10)  Solid state

**Caution:** The "Minimum" values apply to systems running base system content at low EPS (typical in lab environments). It should not be used for systems running high number of customer-created resources, or for systems that need to handle high event rates. Use the "Mid Range" or "High Performance" specifications for production environments that handle a sizable EPS load with additional content and user activity.

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

If you anticipate that you will have large lists (a list with roughly five million entries) or 500,000 Actors, ensure that your system meets the Mid-Range requirements or better.

## Supported Platforms

ESM 6.8c is supported on Red Hat Enterprise Linux 6.4 and 6.5 and CentOS 6.5 and SUSE Linux Enterprise 11 SP3 platforms (all 64-bit) installed using at least the "Basic Server" option with added "compatibility libraries" at the time of installation. Refer to the Product Lifecycle document available on the Protect 724 site for further information on supported platforms and browsers.



**Note:**

- To install the product you may also install the X Window system package if it is not already installed. This is optional. Use `xorg-x11-server-utils-7.5-13.el6.x86_64` or a later version for RHEL. Use `xorg-x11-server-7.4-27.81.7` or a later version for SUSE Linux.
- For RHEL, the XFS and EXT4 file system formats are supported.
- For SUSE Linux, the EXT3 file system format is supported.
- The `atd` service must be running all the time. At the end of the ESM installation, if the service is not already running, it starts when you run the `setup_services.sh` command.
- If you plan to use this instance of ESM with the HA Module, do not use SUSE Linux; the HA Module does not support SUSE Linux.

## Before you Install ESM

Before you begin to install ESM, do the following:

- The ESM 6.8c installation package is available for download from HP at <https://softwaresupport.hp.com/>. Download the `ArcSightESMSuite-6.8.0.xxxx.0.tar` file and copy it on to the system where you will be installing ESM. The `xxxx` in the file name stands for the build number.
- After you download the `.tar` file from the HP Software Depot, initiate license procurement by following the instructions in the Electronic Delivery Receipt you receive from HP in an email after placing the order.

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

- If you plan to install the Risk Insight software with ESM, create a new partition with at least 25 GB for it in addition to the space allocation you make for ESM.  
Consult the *ArcSight Risk Insight Deployment Guide* for details.

## Keep these TCP Ports Open

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

Open the following TCP ports for external incoming connections:

8443  
9443  
9000

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

1976, 28001, 2812, 3306, 5555, 6005, 6009, 6443, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8766, 8808, 8880, 8888, 8889, 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9095, 9090, 9123, 9124, 9999, 45450

If you are using the ESM High Availability Module, check its documentation for ports that it uses.

## Install Time Zone Package

ESM uses the time zone update package in order to automatically handle changes in time zone or changes between standard and daylight savings time. During installation, ESM checks to see if the appropriate operating system time zone package is installed. If it is not, you have the option of exiting the installer to install the latest operating system timezone update or continuing the ESM installation and skipping the timezone update for ESM components. We recommend installing the time zone update package.

- For RHEL 6.4/6.5 and CentOS 6.5 use `tzdata-2014f-1.el6.noarch.rpm`.
- For SuSE 11.x use `timezone-2014f-8.1`.  
When installing the timezone package on SuSE, some dependencies need to be resolved. Please check with your system administrator if you have a problem resolving these dependencies.

In both cases, the "f" can be f or any later version. To install them use the command:

```
rpm -Uvh <package>
```

You should also check to make sure that the `/etc/localtime` link is pointing to a valid time zone. To do that, run the following command:

```
ls -altrh /etc/localtime
```

You should get a response similar to this (below), where `<ZONE>` is your time zone such as `America/Los_Angeles`.

```
lrwxrwxrwx. 1 root root 39 Nov 27 08:28 /etc/localtime ->
/usr/share/zoneinfo/<ZONE>
```

If this is not correct, run the following commands as user `root`:

```
source /etc/sysconfig/clock
mv /etc/localtime /etc/localtime.old
ln -s /usr/share/zoneinfo/<ZONE> /etc/localtime
```

Verify that `/etc/localtime` is pointing to the correct time zone or use the `date` command.

If you quit the installation to fix these, you can simply run the installation again.

If you complete the installation without fixing these, you can still set up the time zone package after completing the installation. Use the following procedure (after ensuring that you have downloaded and installed the correct package and the link is set correctly):

1. As user *arcsight*, shut down all arcsight services. (This is important.) Run  
`/opt/arcsight/services/init.d/arcsight_services killAllFast`

2. As user *root*, run the following command (this is one line):

```
/opt/arcsight/manager/bin/arcsight tzupdater /opt/arcsight /opt/arcsight/manager/lib/jre-tools/tzupdater
```

3. Monitor for any failure.

4. Restart all arcsight services.

## Preparing to Install

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

## Set the /tmp Directory Size

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

## Sizing Guidelines for CORR-Engine

When installing ESM 6.8c, the default CORR-Engine storage sizes are automatically calculated based on your hardware according to the default values in the table below. These are the recommended sizing guidelines. You can change any of the default storage sizes in the “CORR-Engine Configuration” panel of the wizard, but when doing so, be sure that you take the minimum and maximum values allowed into consideration.

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

**Event Storage** - storage for events

**Online Event Archive** - archive of online events

	Recommended	Minimum	Maximum
<b>System Storage Size</b>	Specify about one-sixth of calculated usable space. Usable space is shown on the CORR-Engine Configuration panel during installation.	3 GB	500 GB
<b>Event Storage Size</b>	Specify about two thirds of the usable space shown during installation.	10 GB	12 TB

	Recommended	Minimum	Maximum
<b>Event Archive Size</b>	You may specify the remaining space after the System and Event storage have been allocated.	1 GB	No limit

The system reserves 10 percent of the /opt/arcsight partition for its own use.

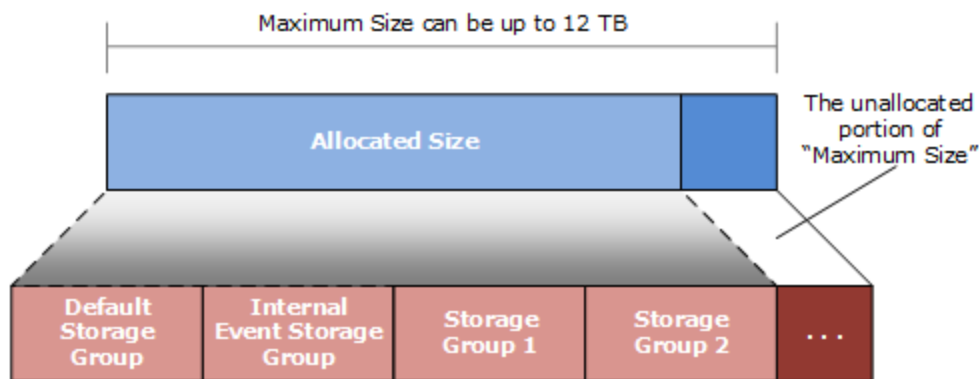
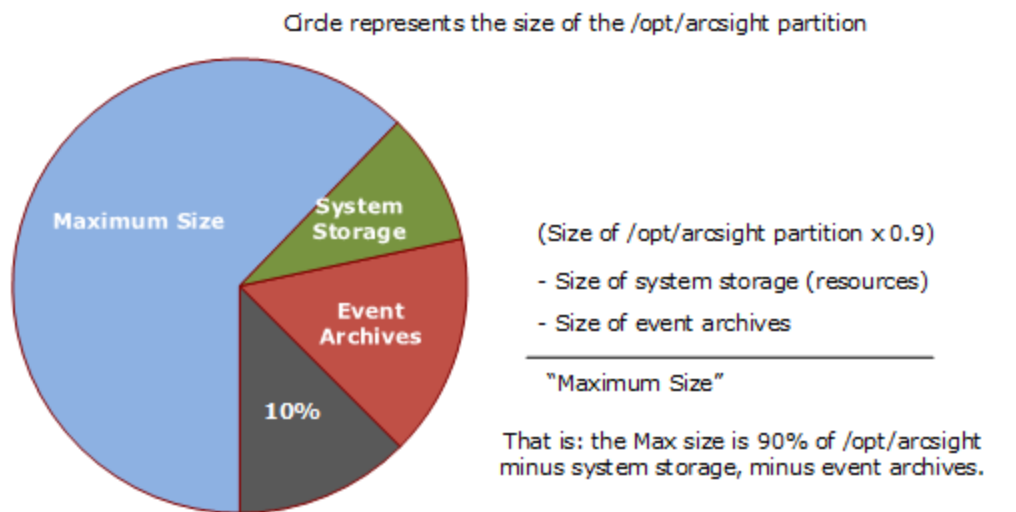
During installation, the system will show the size of the /opt/arcsight partition as "Available Space," and the size of that partition less 10 percent reserved space as "usable Space." The maximum event storage volume size is calculated by the system using this formula:

Maximum Event Storage = /opt/arcsight partition x 0.9 - system storage - event archives.

After installation, the allocated event storage space consists of a default storage group and an internal storage group whose size is initially set by the installer. These storage groups do not fill the maximum size of the event storage volume. You may expand the size of these storage groups or add up to four of your own storage groups until the allocated size of the event storage reaches the maximum size of the event storage volume. Use the ArcSight Command Center user interface to add or change the size of storage groups.

In the ArcSight Command Center, select **Administration > Storage and Archive** to see and change the storage allocations. Refer to the *ArcSight Command Center User's Guide* for details.

The following diagrams clarify the various terms used in the configuration wizard and in the ArcSight Command Center user interface:



You can add up to four of your own storage groups and expand any of them to increase the Allocated Size until it reaches the Maximum Size.

## Create User *arcsight*

You can skip this step if you are installing the ESM High Availability Module and already created this user and group as part of the HA Module planning and installation.

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

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

Change the password for user *arcsight*:

```
passwd arcsight
```

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

Make sure that the `useradd` operating system command successfully created a file in `/home/arcsight` called `.bash_profile`. If the operating system does not create this file, the installation will fail. If the file is not created, consult your operating system administrator.

## Create `/opt/arcsight` Directory

ESM 6.8c is installed in `/opt/arcsight/`. If the `/opt/arcsight/` directory does not exist, create it while logged in as a `root` user.

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

Change the owner and group of `/opt/arcsight/` to the `arcsight` user and group by issuing the following commands while logged in as `root`:

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

## Increase User Process Limit

The operating system's default user process limit is not necessarily sufficient. This may cause an error when the Manager tries to create more threads. To ensure that the system has adequate processing capacity, increase this default limit, while logged in as user `root`:

1. If you do not already have a file `/etc/security/limits.d/90-nproc.conf`, create it (and the `limits.d` directory, if necessary).

If the file already exists, delete all entries in the file.

2. Add the following lines:

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

**Caution:** Be sure to include the asterisk (\*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system runtime errors.

3. Reboot the machine.
4. Log in as user `arcsight`.
5. Run the following command to verify the new settings:

```
ulimit -a
```

6. Verify that the output shows the following values for Open files and Max user processes:

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

## Untar the tar File

**Note:**

- Using an `ssh -X` session to run the ESM 6.8c installation file causes errors and the wizard does not complete. Instead of using `ssh -X` to run the installation wizard, use `ssh` to connect to the machine where you will be installing ESM 6.8c and set your `DISPLAY` environment variable to point to a valid X11 display.
- Spaces in directory names appearing within paths are not supported.

1. Untar the tar file in order to obtain the installation file. To do so:
  - a. Log in as user *arcsight*.
  - b. Transfer the license file and the `.tar` file to this machine since you will be installing ESM on it.

**Important!**

The `.tar` file should be owned by the user *arcsight*.

- c. Change directory to the location where you downloaded the `.tar` file.
- d. Run the following command to untar the file:

```
tar xvf ArcSightESMSuite-6.8.0.xxxx.0.tar
```

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

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

## Running the Installation File

Start the installation while logged in as user *arcsight*.

1. Run the following command:

```
export LC_ALL=[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)

2. Run the installation file as follows:

```
./ArcSightESMSuite.bin
```

(or `./ArcSightESMSuite.bin -i console`, for console mode.)

The installation wizard opens.

**Note:**

- To run in GUI mode, X Windows must be running. If it is not, the installer automatically runs in Console mode.
- To run in Console mode, make sure X Windows is *not* running. Console mode requests the same information as GUI mode and is not documented separately.
- The log files for this installation appear in the `/home/arcsight` directory.

3. Read the **Introduction** message 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 reading the License Agreement, click the **I accept the terms of the License Agreement** radio button and click **Next**.
5. Read the **Special Notice** and click **Next**.
6. On the **Choose Link Folder** panel, select the location where you would like the installer to place the links for this installation and click **Next**.
7. Review the **Pre-Installation Summary**. If need be, click **Previous** to make any changes. When you are ready to proceed, click **Install**.

The **Installing ArcSight ESM 6.8c Suite** screen appears with a progress bar at the bottom.

8. The installer first places all the installation files in the appropriate folders. When it is done, the **File Delivery Complete** screen opens. Click **Next**.

The Suite Installer installs each component. After the GUI completes, the Configuration Wizard GUI opens automatically. See ["Running the Configuration Wizard In Console Mode" on the next page](#) for details on configuring ESM.



## Rerunning The Suite Installer

If the installation is interrupted and the process exits (for any reason) before you get to "File Delivery Complete:"

1. Remove all `install.dir.xxxx` directories from the `/tmp` directory.
2. Remove all directories and files in the `/opt/arcsight` directory.
3. Rerun the installer.

## Running the Configuration Wizard In Console Mode

If you are using the GUI mode (as instructed above) to install ESM, skip this topic and go to ["Configuring ESM" below](#). If you started installing ESM in console mode (from the command line), the installation stops at this point when the Suite Installer is done, but it does not automatically continue with the Configuration Wizard. You will explicitly need to start the configuration wizard manually by issuing the following command:

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

## Configuring ESM

Once the Suite Installer (GUI) completes, the Configuration Wizard opens automatically.

### Note:

If you run the installer in console mode via the command line, you have to manually start the wizard. See ["Running the Configuration Wizard In Console Mode" above](#) for details on how to do this.

1. Read the Welcome screen and click **Next**.
2. On the **Language Options** panel, select the language for interface displays and click **Next**.
3. On the **CORR-Engine Password** panel, set a password for the CORR-Engine and reenter it in the Password confirmation text box and click **Next**. For information on password restrictions, see the Administrator's Guide for ESM, chapter "Configuration", section "Managing Password Configuration".
4. On the **CORR-Engine Configuration** panel, enter the CORR-Engine storage allocation information and click **Next**.

**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

5. On the **Notification Emails** panel, Configure the following e-mail addresses:

**Error Notification Recipients:** The email address of the person 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.

Click **Next**.

6. On the **License File** panel, Enter or browse to the location of the license file you downloaded. Click **Next**.

If you have a valid existing ESM license, you can use it with ESM6.8c.

7. On the **Manager Information** panel, enter the Manager's hostname or IP address and set a password for the admin user and click **Next**.



The screenshot shows the 'ESM v6.8c Configuration Wizard' window. On the left is a vertical navigation pane with the following items: Introduction, Language, CORR-Engine, Notification Email, **Manager** (highlighted in red), Configuration, and Complete. The main area is titled 'Manager Information' and contains the following text: 'Provide ArcSight Manager host name (recommended) or IP address, and Administrator login credentials.' Below this is a note: 'If you choose to provide a host name here, make sure it can be resolved through your Domain Name System (DNS) server.' There are four input fields: 'Manager host name (or IP)' with a placeholder '<hostname>', 'Administrator user name' with the value 'admin', 'Administrator password' with masked characters '\*\*\*\*\*', and 'Password confirmation' with masked characters '\*\*\*\*\*'. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

**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 talk to the Manager. Using a host name and especially a fully-qualified domain name instead of an IP address is recommended for flexibility.

The Manager host name 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.

8. On the **Foundation Packages** panel, check the system content packages to install. The System Content is delivered in the form of packages. System content packages are automatically installed as a part of ESM to provide out-of-box resource suites that you can use immediately to monitor and protect your network.

By default, it installs the ArcSight Administration package that provides you information about this ESM instance. You can select other packages to install from the list.

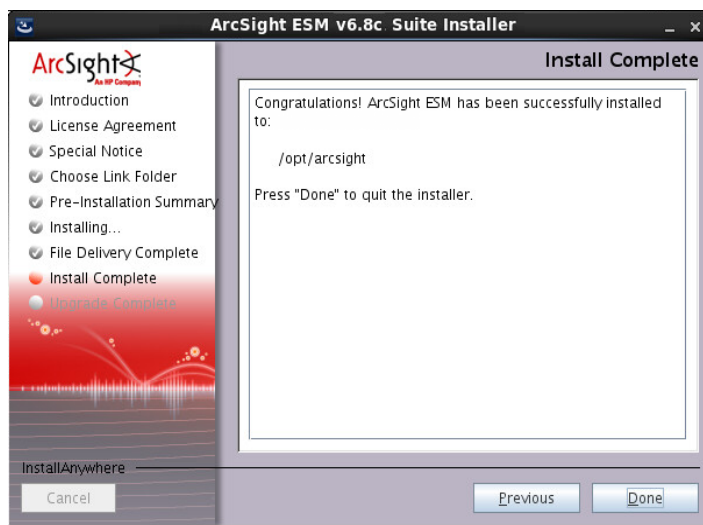
For more information about packages, see the *ESM System Content Guide*.

9. The next screen is **About to Configure ESM 6.8c**. It informs you of the ESM configuration steps it will perform when you click **Next**.

**Caution:** Review the selections you made in the previous screens of this wizard and make sure that they are to your satisfaction. Once you click Next, the product is installed as specified.

If you are satisfied, click **Next**.

10. Upon successful configuration, the **Configuration Completed Successfully** screen appears. Click **Finish**.
11. Click **Done** on the **Install Complete** screen.



12. **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.

## Handling a Time Zone Update Error

There are two possible errors that can happen when the installer tries to update the time zone information for the ESM components.

1. A timezone version 2014f or later rpm for your operating system is not installed.
2. The `/etc/localtime` link is pointing to invalid or non-existent timezone.

You can choose to continue with the installation even if the right timezone package is unavailable or incorrectly setup. If you choose to do so, you can update timezone info for the ESM components post-installation. Refer to ["Install Time Zone Package" on page 18](#), to correct one of these time zone issues.

## Changing the Manager Heap Size

If you need to change the Manager's heap size after the installation completes, you can do so from the ArcSight Command Center. Refer to the *ArcSight Command Center User's Guide* for further details.

## Rerunning the ESM Configuration Wizard

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 v6.8c". See ["Rerunning the ESM Configuration Wizard" below](#) for details.

## Rerunning the ESM Configuration Wizard

You can rerun the wizard manually only if you exit it at any point **before** you click Next on the screen called "About to Configure ESM <version>".

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

1. To rerun the wizard run:

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

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

### In GUI mode

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

### In console mode

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

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

If you encounter a failure during the configuration stage, uninstall and reinstall ESM.

## Uninstalling ESM

Use the following procedure to uninstall ESM.

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

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

3. Log in as user *arcsight*.
4. Shut down any *arcsight* processes that are still running.

To check for running *arcsight* processes, run:

```
ps -elf | grep "/opt/arcsight"
```

To shut down any *arcsight* processes that are running, run:

```
kill -9 <process_id_number>
```

5. Run the uninstaller program from either the directory where you have created the links while installing the product or if you had opted not to create links, then run this from the `/opt/arcsight/suite/UninstallerData` directory:

```
./Uninstall_ArcSight_ESM_Suite_6.8
```

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

```
./Uninstall_ArcSight_ESM_Suite_6.8
```

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

## 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 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 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.

## Improving the Performance of Your Server

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

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

This setting changes the following:

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

## The Next Steps

Download the ArcSight Console and install it on a supported platform. Refer to the chapter on installing the Console, for details on how to do this. You can also access the Manager from the ArcSight Command Center using a browser. To do so, enter the following URL in the browser's address bar:

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

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

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



## Chapter 3: Installing ArcSight Console

The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of the ArcSight Command Center) to ArcSight ESM. This chapter explains how to install and configure the ArcSight Console in default mode.

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

### Console Supported Platforms

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

### Required Libraries for RHEL and CentOS (64 Bit)

On the RHEL and CentOS 6.5 64-bit workstations, the Console requires the latest versions of following libraries, if available:

```
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
```

## 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 supports the use of a PKCS#11 token such as the Common Access Card (CAC) 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."

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

## Installing the Console

**Note:** This box includes several important notes related to Installing the ArcSight Console.

On Macintosh platforms, please make sure that:

- You are using an intel processor based system.
- You have the JRE installed on your system before installing the Console. Refer to the Release Notes for the version of JRE to install.
- If you are installing the Console on a new system for the first time, or if you have upgraded your system causing the JRE update, your Console installation might fail. To work around this, change the permissions on the cacerts file to give it write permission before you import it.
- If your JRE gets updated, you will see the following error when you try to log into the Console: `IOException: Keystore was tampered with or password was incorrect.`

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

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

Do not attempt to install the Console as the root user on Unix-based machines. If you do, the installer will prompt 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.

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

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-6.8.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-6.8.x.nnnn.y-Console-Win.exe
Macintosh	ArcSight-6.8.x.nnnn.y-Console-MacOSX.zip

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

Platform	Installation Log Files
Linux	/home/<user>
Windows	C:\Users\<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:** On Linux and Macintosh systems, spaces are not supported in install paths.

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.

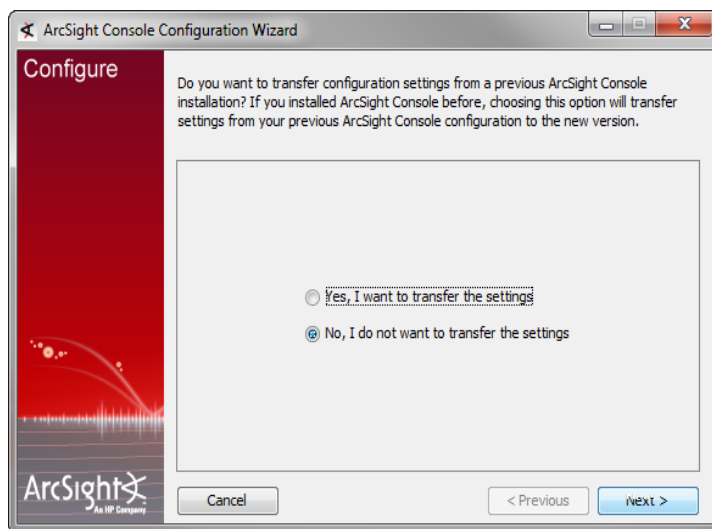
You can view the installation progress in the progress bar.

**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.tzdata2014b\ 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.

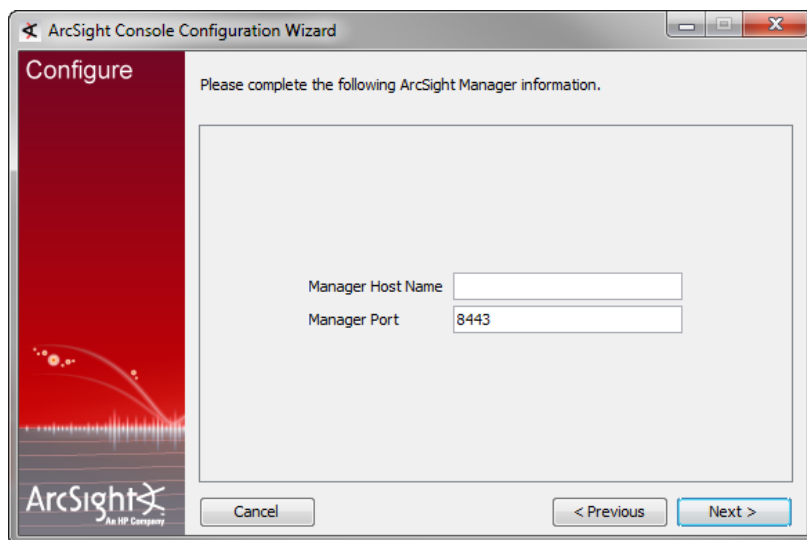
1. The wizard asks if you would like to transfer configuration options from an existing installation of ArcSight Console. Choose **No, I do not want to transfer the settings** to create a new, clean installation and click **Next**.



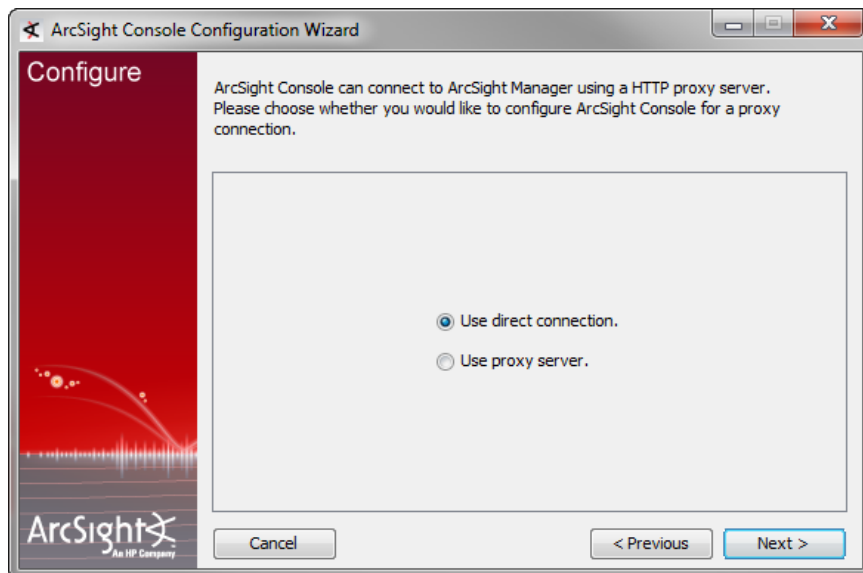
2. Enter the host name of the Manager to which the Console will connect.

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

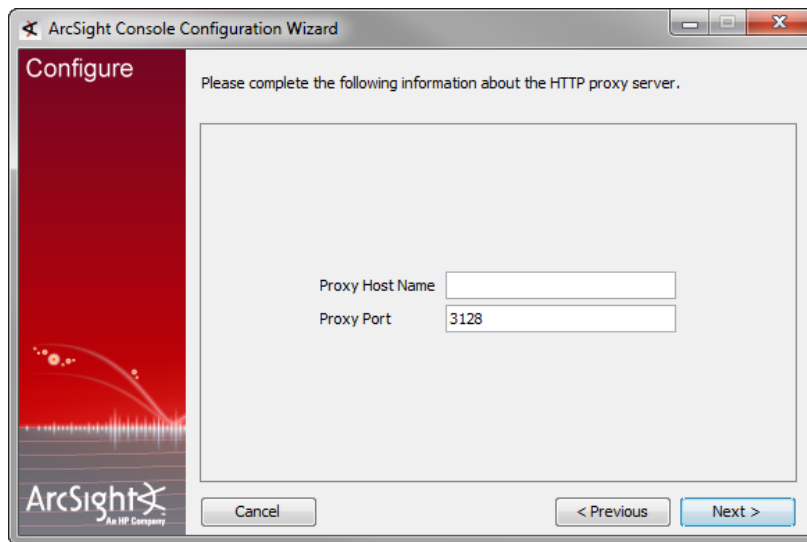
Click **Next**.



3. 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.



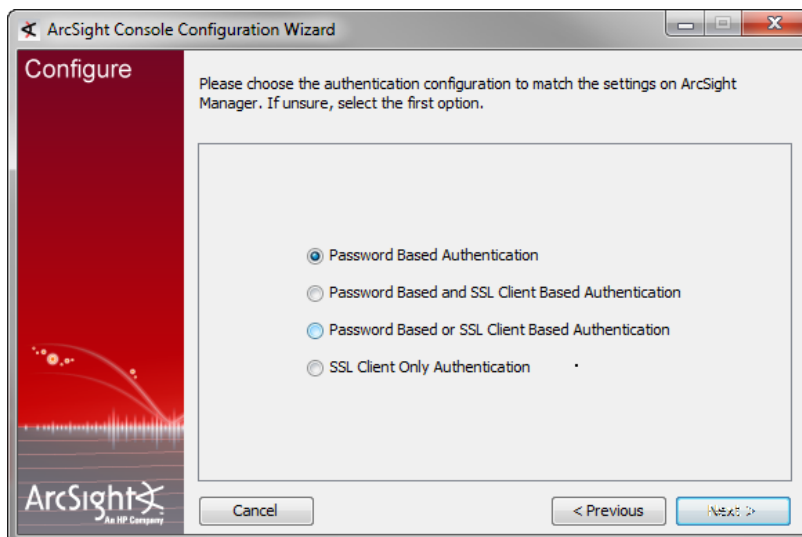
If you select the Use proxy server option, you will be prompted to enter the proxy server information.



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

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

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

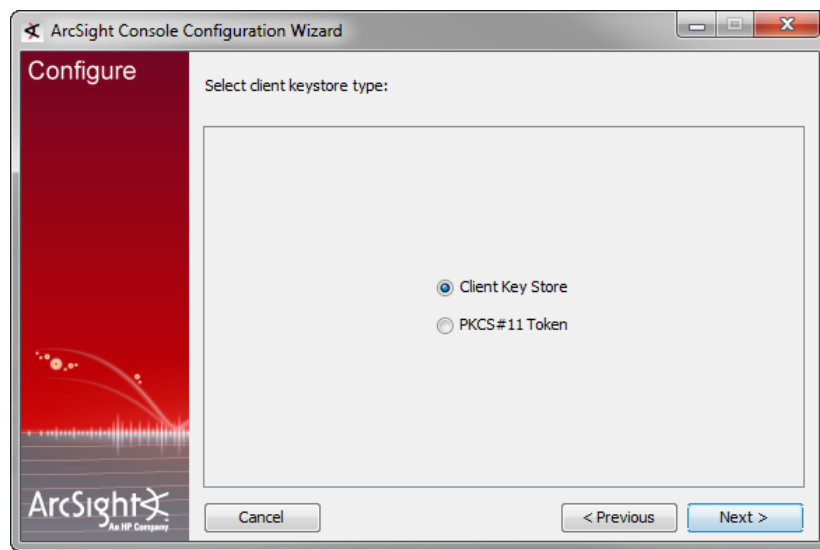


**Note:** **Password Based and SSL Client Based Authentication** option currently supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method within the **Password Based and SSL Client Based Authentication** option is not currently supported.

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

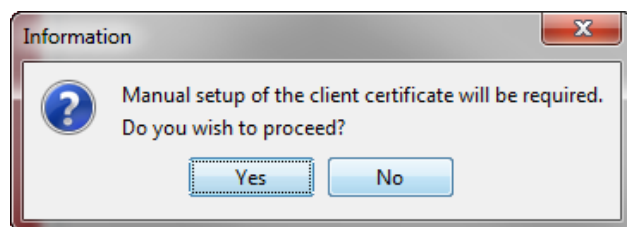
If you select **Password Based and SSL Client Based Authentication**, you need a client certificate to log in, in addition to your user name and password. Follow the procedure described in ESM Administrator's Guide to set up the client certificate.

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.



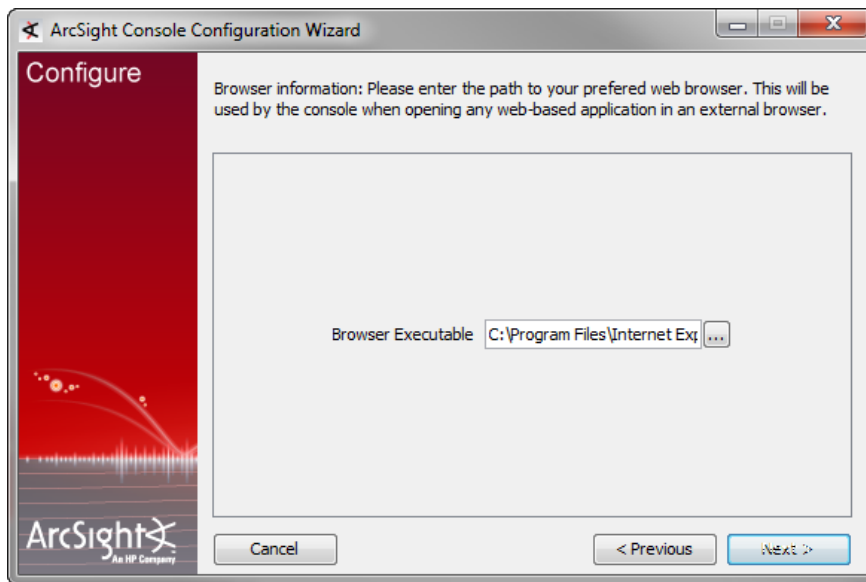
If you plan to use a PKCS #11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the Console, you can refer to ["Setting Up to Use a CAC Card " on page 60](#) 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.

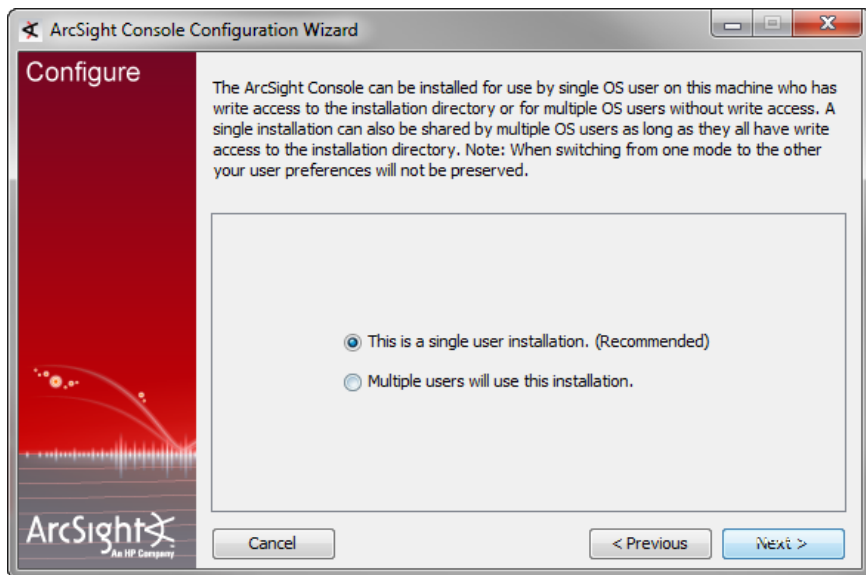


After completing the Configuration Wizard, follow the procedure described in ESM Administrator's Guide to set up the client certificate.

5. The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Centered Support articles, and other web page content. Specify the location of the executable for the web browser that you want to use to display the Knowledge Centered Support articles and other web pages launched from the ArcSight Console. Click **Next**.



6. 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

Select this option when:

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



OR

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

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

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

- Multiple system users will use this installation

Select this option when:

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

AND

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

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

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

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

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

- sendlogs
- console
- exceptions
- portinfo
- websearch

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

**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, 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

`C:\<ARCSIGHT_HOME>\current\jre\lib\zi.tzdata2014b`

match the date and time when you installed the Console. (The `b` in `tzdata2014b` could be a different letter.) If the time stamp is older or the files are missing, finish the next two steps, then uninstall and re-install the Console.

7. You have completed configuring your ArcSight Console. Click **Finish** on the final panel to close the configuration wizard.
8. Click **Done** in the next screen.
9. If you are installing the Console on a Linux machine in a different language than the machine on which the Manager is installed, edit the file `/home/arcsight/.bash_profile` by adding the line:

```
export LC_ALL=[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 an browser if you are using SSL Client Based Authentication mode:

1. Export the keypair from the Console. Refer to the ESM Administrator's Guide for in the "Using Keytoolgui to Export a Key Pair" section.

2. Import the Console's keypair into the browser.

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

## Character Set Encoding

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

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

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

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

If you must use a non-UTF-8 encoding, and you must have user IDs with other characters in them, 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 ARCIGHT\_JVM\_NET\_OPTIONS.

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

### On Unix

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

### On Windows set

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

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

## Logging into the Console

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

To start the Console, click **Login**. When you start the Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the Manager's certificate. The prompt will show details specific to your settings. 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 6.8c Console > Uninstall ArcSight ESM Console 6.8c** program. If a shortcut to the Console was not installed on the Start menu, locate the Console's UninstallerData folder and run:

```
Uninstall_ArcSight_ESM_Console_6.8c.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:

```
./Uninstall_ArcSight_ESM_Console_6.8c
```

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

```
./Uninstall_ArcSight_ESM_Console_6.8c
```

**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 <a href="#">"Configuring ESM" on page 25.</a>
firstbootsetup.log	/opt/arcsight/manager/logs/	Contains brief troubleshooting information about commands that ran during the steps in <a href="#">"Configuring ESM" on page 25.</a>
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
<b>Manager Log Files</b>		
server.log	/opt/arcsight/manager/logs/default	Contains troubleshooting information about the Manager
server.std.log	/opt/arcsight/manager/logs/default	Contains the stdout output of the Manager
server.status.log	/opt/arcsight/manager/logs/default	Contains a dump of all the MBeans, the memory status, thread status, etc.
<b>ArcSight Web Log Files</b>		
webserver.log	/opt/arcsight/web/logs/default	Contains troubleshooting information about ArcSight Web



Log file name	location	Description
webserver.std.log	/opt/arcsight/web/logs/default	Contains the stdout output of ArcSight Web
server.status.log	/opt/arcsight/web/logs/default	Manager status monitoring log file
<b>Log file for services</b>		
arcsight_services.log	/opt/arcsight/services/logs/	Contains information from commands that manage ArcSight service processes.
monit.log	/opt/arcsight/services/monit/data/	Contains timing information from startup and shutdown of ArcSight service processes.

## If You Encounter an Unsuccessful Installation

If you encounter an unsuccessful installation, or if your installation is corrupted, there are two possible cases.

**Case 1** – If your installation became corrupted after running `setup_services.sh`, run the following script as root user:

```
remove_services.sh
```

Then run the Recovery procedure below.

**Case 2** – If your installation became corrupted before running `setup_services.sh`, run the recovery procedure.

**Recovery Procedure** – Run this for either case 1 or case 2, above.

1. Kill any ArcSight services that are currently running. Either:
  - a. Run:

```
/opt/arcsight/services/init.d/arcsight_services killAllFast
```
  - Or

- b. Query if there are any ArcSight processes running and manually kill them.
2. Delete all ArcSight-related files/directories under `/opt/arcsight` and `/tmp` directory.
3. Delete any shortcuts created during installation (by default in the home directory of the *arcsight* user).
4. Re-install the product.

## Customizing ESM Components Further

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:

### ArcSight Manager

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
```

### ArcSight Web

While logged in as user *arcsight*,

1. Stop ArcSight Web if it is running:  
  

```
/etc/init.d/arcsight_services stop arcsight_web
```
2. Run the following command from `/opt/arcsight/web/bin` directory:

```
./arcsight webserversetup
```

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

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

## Fatal Error when Running the First Boot Wizard

If you encounter a fatal error while running the First Boot Wizard, the wizard will display an error message and then exit. Check the log files for the particular component for any error messages. The log files are listed in the section ["Location of Log Files for Components" on page 47](#).

To resolve this issue, try the following steps:

1. Check the `/opt/arcsight/manager/logs/default/fbwizard.log` file to figure out where the error occurred.
2. Check to make sure that all the required TCP ports mentioned in the section ["Keep these TCP Ports Open" on page 17](#) are open.
3. The First Boot Wizard can only be rerun if it did not reach the point where it configures the Manager. See section ["Rerunning the ESM Configuration Wizard" on page 29](#) for more details on this. If your error occurred before any component got configured, restart the First Boot Wizard by running the following command from the `/opt/arcsight/manager/bin` directory when logged in as user "arcsight":

In GUI mode:

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

In console mode:

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

## Changing the Hostname of Your Machine

Wherever you see "hostname," you may assume it means "hostname or IP address." If you have configured peering, make sure to re-establish the peer relationship.

If you are using the High Availability module, the procedure is different. Refer to the *ArcSight High Availability Module User's Guide* for the proper procedure.

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

**Note:** Run the Manager setup command when logged in as user *arcsight*.

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

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

2. Change the hostname 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*, stop ArcSight Web by running:

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

You might get error messages from this command indicating that ArcSight Web was not stopped. This is normal and you should ignore it.

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

```
./arcsight managersetup
```

- a. Enter the new host name (that you set for your machine in the steps above), in the Manager Host Name field when prompted by the wizard – and in every other field where the old hostname is displayed.
- b. Make sure to select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new host name.

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

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

8. As the user *arcsight*, see if the manager is running yet by running the command.

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

Run this command about once a minute, until you see the line "manager service is available." Then you can continue with the next step.

9. As user *arcsight*, run the following to start the setup program for ArcSight Web from the `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

- a. Enter the new host name in **Webserver Host Name** field and every other field containing the old host name when prompted.
  - b. When the certificate from the manager is displayed, check the option “Trust the certification from the manager.”
  - c. Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new hostname.
10. As the user *arcsight*, start ArcSight Web by running:  

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

You may ignore the message indicating that ArcSight Web is already started.
11. Wait two minutes to ensure that ArcSight Web has started.
12. Import the Manager’s newly-generated certificate on all clients (Console and connectors) that access the Manager. Use keytoolgui. See the “Using Keytoolgui to Import a Certificate” section in the “Configuration” chapter in the ESM Administrator’s Guide available on the HP ArcSight Customer Support download site for details.
13. Test to make sure that
  - The clients can connect to the Manager
  - Peer configuration works as expected. If not, redo the peer configuration.

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

If you are using the High Availability module, the procedure is different. Refer to the *ArcSight High Availability Module User’s Guide* for the proper procedure.

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

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

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

```
/etc/init.d/arcsight_services stop all
```
2. Change the host name of your machine.
3. Reboot the machine.

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

1. As the user *arcsight*, stop the Manager by running:

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

2. As the user *arcsight*, stop ArcSight Web by running:

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

3. 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 (that you set for your machine in the steps above), in the Manager Host Name field when prompted by the wizard.
- b. Make sure to select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new host name.

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

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

5. Export the Manager's newly generated self-signed certificate and import it into ArcSight Web using the `keytoolgui` tool. For details on how to do this, see the "SSL Certificate Tasks" section in the "SSL Authentication" chapter of the *Administrator's Guide* available on the HP ArcSight Customer Support download site.

6. As the user *arcsight*, run the following to start the setup program for ArcSight Web from the `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

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

7. As the user *arcsight*, start ArcSight Web by running:

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

8. Start ArcSight Command Center by running:

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

Where **<IP address>** is the host name or IP address that you specified when you first configured ESM. (Host names with underscores do not work on IE, so use the IP address.)

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

## 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
Manager Port	8443
Manager license file	
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	changeit
E-mail Notification	<p>Internal SMTP server. If you want to use an External SMTP server,</p> <ol style="list-style-type: none"><li>1. Stop the Manager by running the following command (as user <i>arcsight</i>):  <code>/etc/init.d/arcsight_services stop manager</code></li><li>2. Run the following command from the <code>/opt/arcsight/manager/bin</code> directory and set up the external SMTP server when prompted:  <code>./arcsight managersetup</code></li><li>3. Start the Manager by running (as user <i>arcsight</i>):  <code>/etc/init.d/arcsight_services start manager</code></li></ol>
Sensor Asset Auto Creation	true
Packages/default content installed	Default system content

## ArcSight Web Settings

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

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

## Appendix C: Using 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 supports the use of a PKCS#11 token such as the Common Access Card (CAC) 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."

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 or Common Access Card (CAC). The credentials of the authorized user are stored on the hardware itself. ESM uses the PKCS#11 interface provided by the Network Security Services (NSS) cryptographic module to communicate with it (the NSS cryptographic module). The use of PKCS #11 is an example of client-side authentication.

### PKCS#11 Token Support in ESM

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

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

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

1. Log in to the Command Center.
2. Go to the **Administration** tab.
3. Select **Configuration Management**, on the left.

4. Select **Authentication Configuration**.
5. Select **Password or SSL Client Based** authentication.
6. Restart the ArcSight Manager.

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

## 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. PKCS #12 is applicable to server-side authentication.

## Setting Up to Use a CAC Card

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

1. ["Install the CAC Provider's Software" below](#) on each client machine. That includes the ArcSight Console and every machine using a browser to access ArcSight Web or the Command Center
2. ["Map a User's External ID to the CAC's Subject CN" on the next page](#)
3. ["Obtain the CAC's Issuers' Certificate" on page 63](#)
4. ["Extract the Root CA Certificate From the CAC Certificate" on page 64](#)
5. ["Import the CAC Root CA Certificate into the ArcSight Manager" on page 66](#)
6. ["Select Authentication Option in ArcSight Console Setup" on page 67](#)

## Install the CAC Provider's Software

Before you use the Common Access Card (CAC), make sure that you have installed its software on each client system. That includes the ArcSight Console and any machine with a browser from which you intend to access the Command Center. Refer to your CAC provider's documentation on how to install and configure it.

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

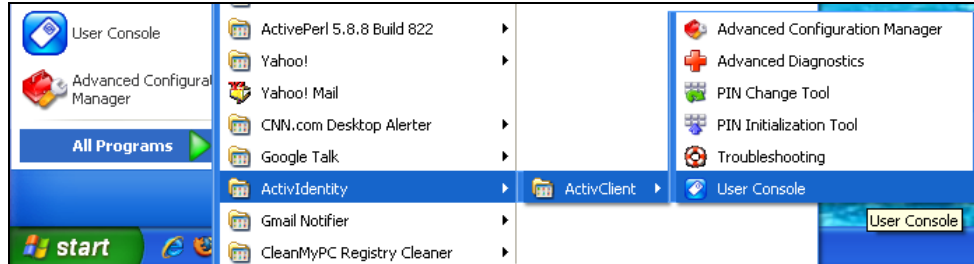
## Map a User's External ID to the CAC's Subject CN

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

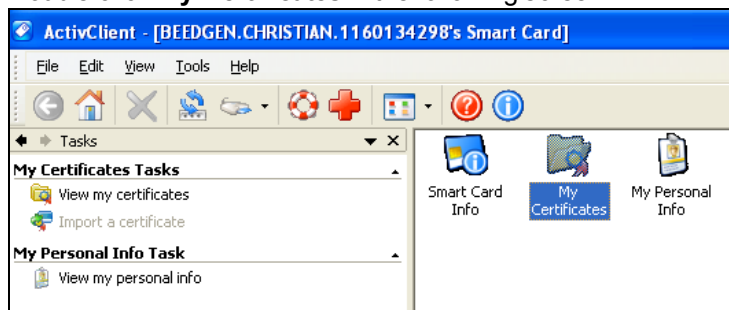
Map the Common Name (CN) on the CAC to a User's External ID on the ArcSight Manager. The external user ID must be identical to the Common Name that appears in the CAC card's ID certificate (include any spaces and periods that appear in the Common name). This allows the ArcSight Manager to know which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

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

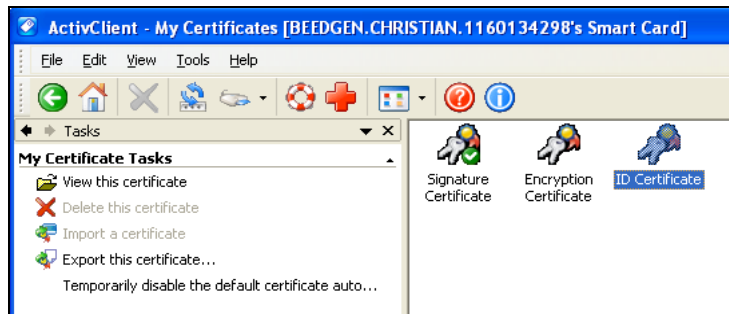
1. Obtain the Subject CN from the CAC card.
  - a. Insert the CAC card into the reader if not already inserted.
  - b. Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



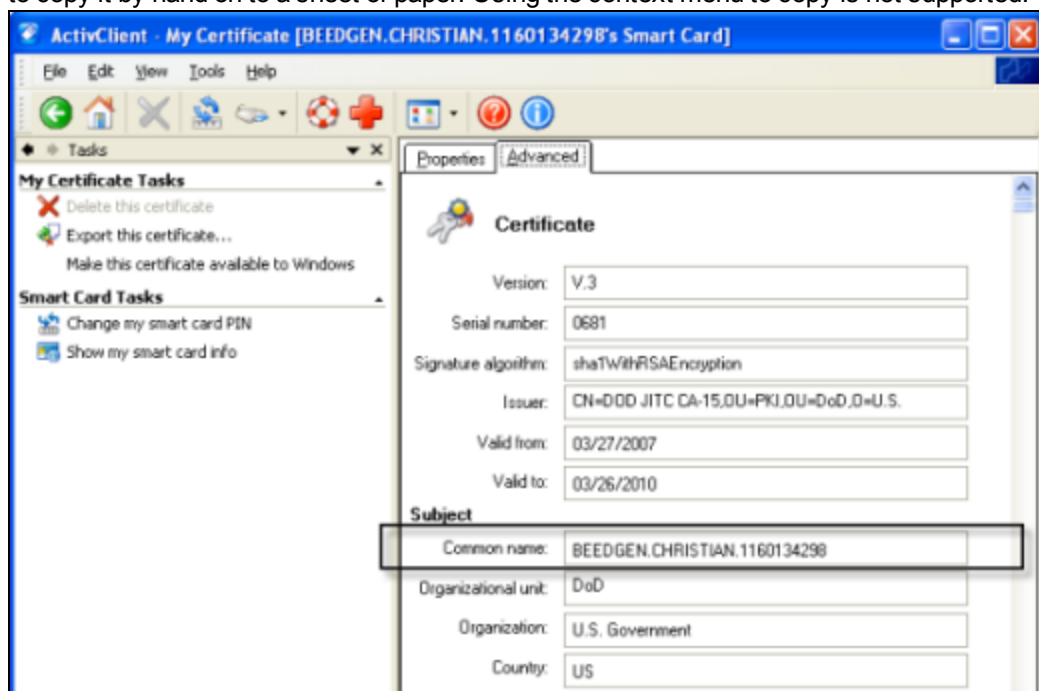
- c. Double-click **My Certificates** in the following screen:



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



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



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

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

- a. In the ArcSight Console, go to **Resources > Users > [user group]** and double-click the user whose External ID you want to map to the CAC 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's Issuers' Certificate

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

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

### Option 1:

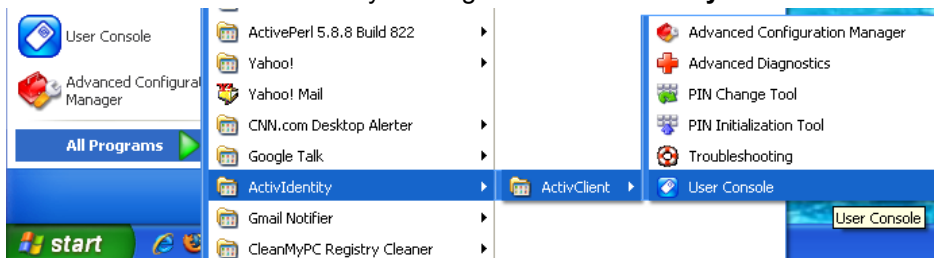
You can obtain the CAC card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

### Option 2:

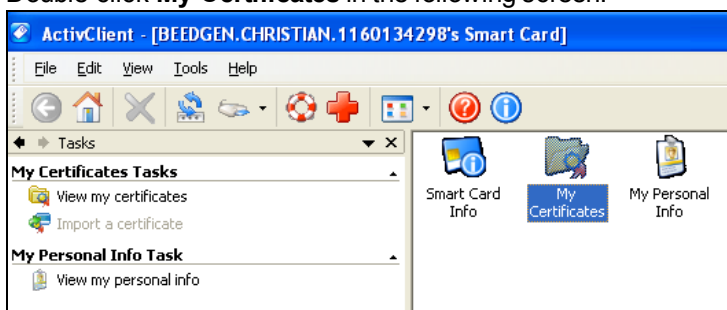
You can export the CAC card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

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

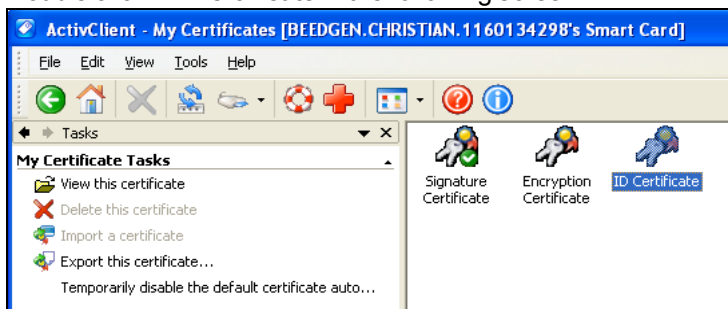
1. Insert the CAC card into the reader if not already inserted.
2. Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



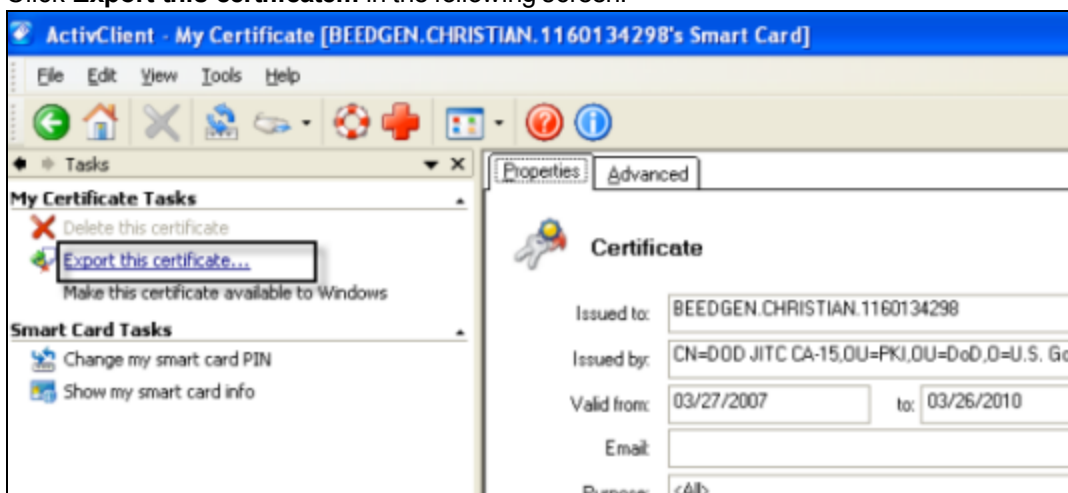
3. Double-click **My Certificates** in the following screen:



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



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



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

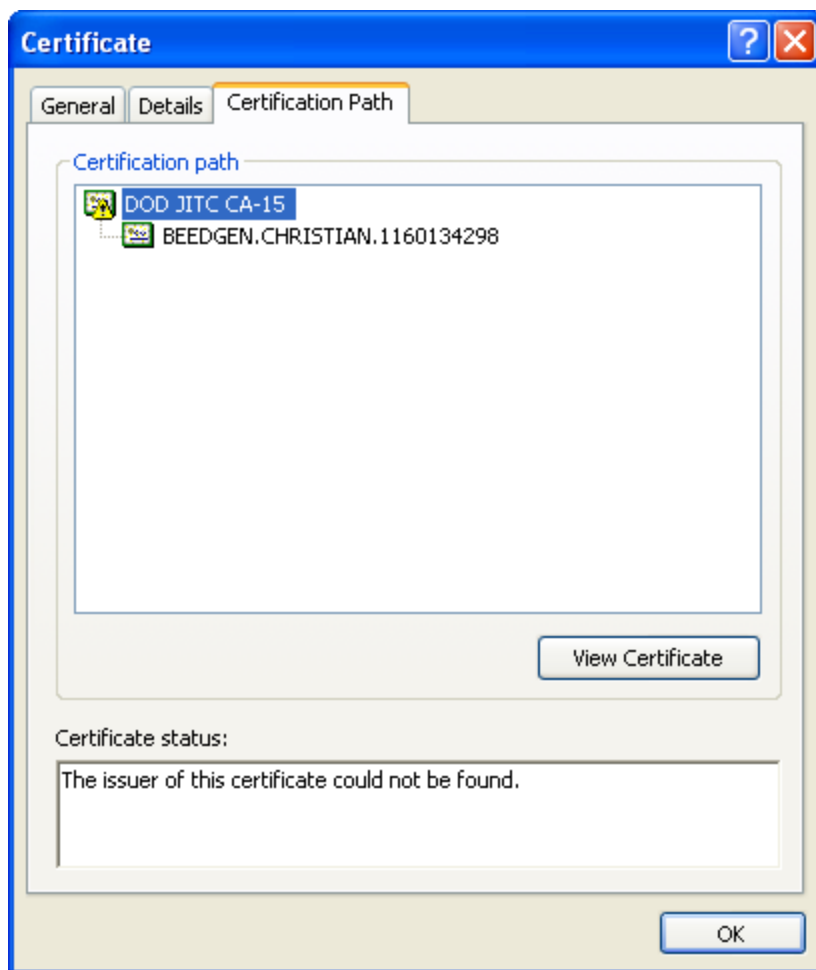
## Extract the Root CA Certificate From the CAC Certificate

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

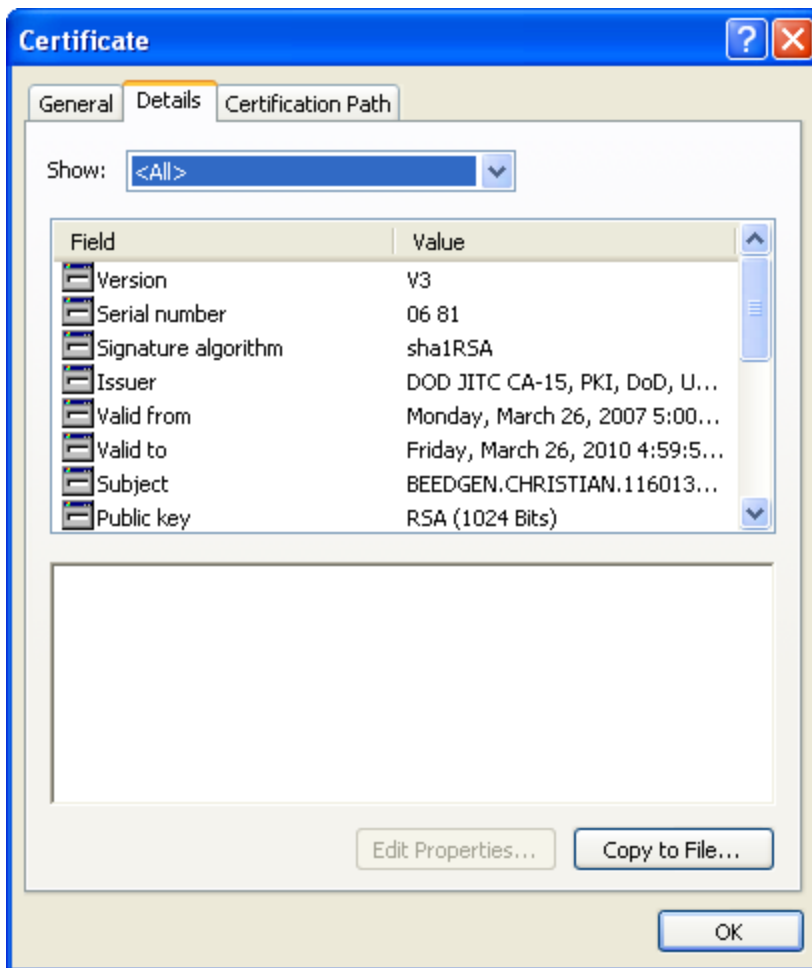
Extract all intermediate certificates too (if any exist) using the following steps:

1. Double-click the CAC's certificate that you exported. The Certificate interface 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 root CA certificate file when prompted and continue with the wizard by accepting all the defaults. The certificate is exported to the same location as the CAC certificate from which you extracted it.
7. Exit the Certificate dialog.

## Import the CAC Root CA Certificate into the ArcSight Manager

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

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

```
./arcsight keytoolgui
```

2. Click **File->Open keystore** and navigate to the truststore 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
```

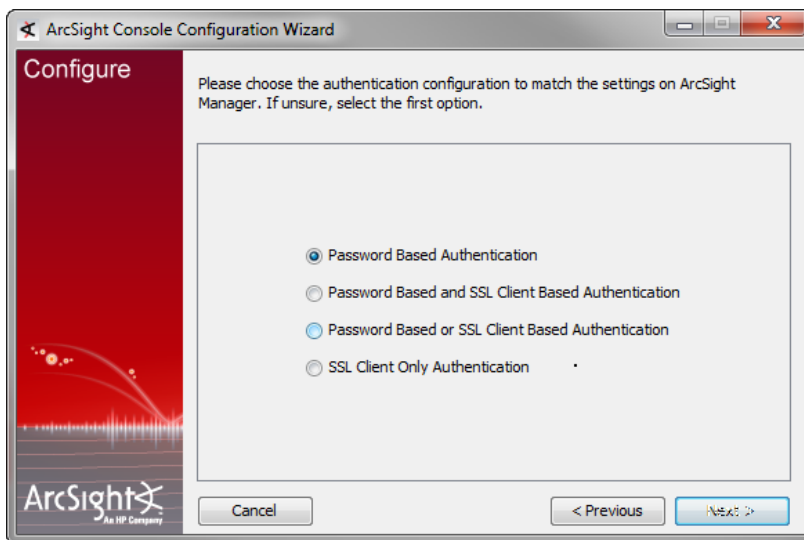
## Select Authentication Option in ArcSight Console Setup

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:

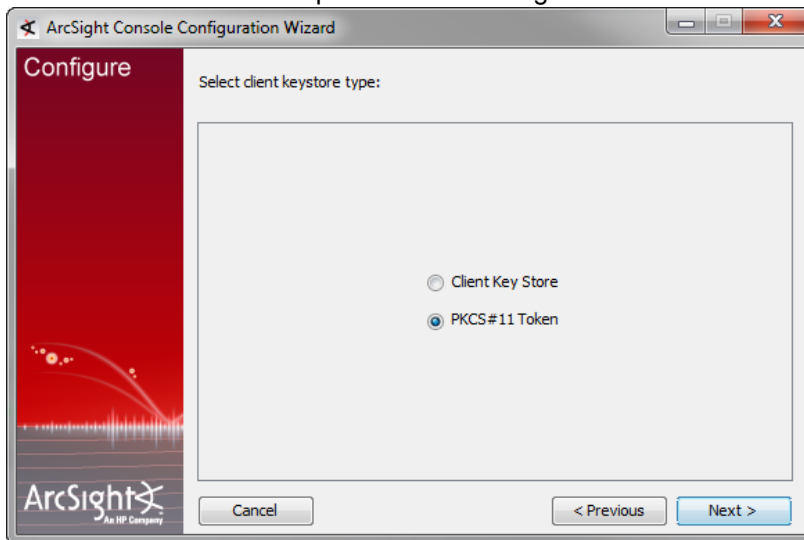
1. Stop the ArcSight Console if it is running.
2. Run the ArcSight Console's setup program from the ArcSight Console's `bin` directory:  

```
./arcsight consolesetup
```
3. Follow the prompts in the wizard screens by accepting all the defaults until you see the screen for the authentication option shown in the next step.

4. Select the authentication that you selected for the ArcSight Manager in the following screen.



5. Follow the prompts in the next few screens by accepting the defaults.
6. Select **PKCS #11 Token** option in the following screen.



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

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

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

On 32-bit Windows:

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

On 64-bit Windows:

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

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

## Logging in to the ArcSight Console Using CAC

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

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

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

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

## Logging in to ArcSight Command Center Using CAC

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

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

If you are using Firefox, be sure to configure Firefox to work with ActivClient by loading the ActivClient module.

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**

## Appendix D: 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, 2014 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	Ukrainian		
uk_UA	Ukrainian	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.

## 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 and Configuration Guide (ESM 6.8c)**

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](mailto:arc-doc@hp.com).

We appreciate your feedback!