Micro Focus Security ArcSight ESM

Software Version: 7.5

Installation Guide

Document Release Date: May 2021
Software Release Date: May 2021

Legal Notices

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

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 different devices on your network and provides you a central, real-time view of the security status of all devices of interest to you. ESM uses the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) storage, a proprietary framework that processes events, and performs searches.

Terminology to Note:

ESM Appliance and ESM Express are different licensing models installed on an appliance.

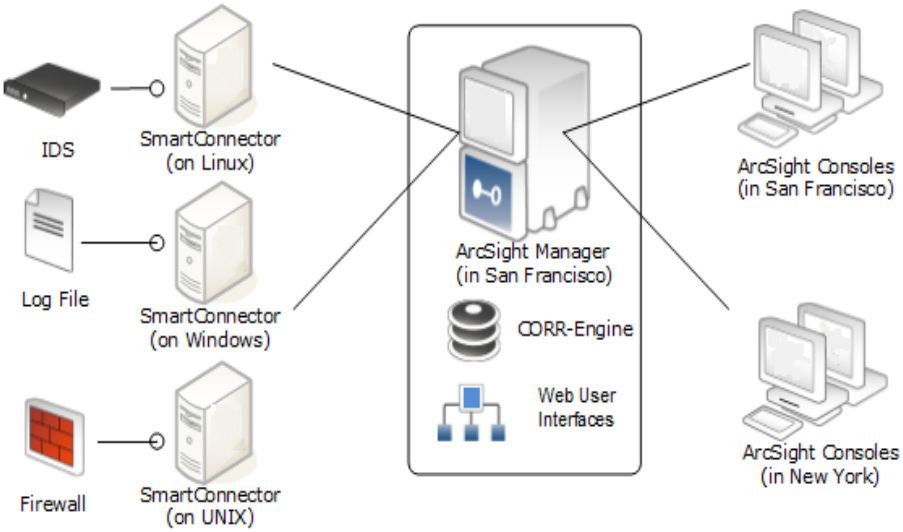
Software ESM is ESM installed on your own hardware.

ESM Basic Components

The ESM system comprises the following components:

- **ESM Manager** -- The Manager is a server that receives event data from Connectors and correlates, reports, and stores them in the database. The Manager and CORR-Engine are integrated components and get installed on the same machine.
- **CORR-Engine** -- The CORR-Engine (Correlation Optimized Retention and Retrieval Engine) is a long-term data storage and retrieval engine that enables the product to receive events at high rates.
- **ArcSight Console** -- The ArcSight Console enables you to perform administrative tasks, such as tuning the ESM content, creating rules, and managing users. The ArcSight Console is installed separately on client machines.
- **ArcSight Command Center** -- The ArcSight Command Center is a web-based user interface that enables you to perform many of the functions found in the ArcSight Console. It provides dashboards, a variety of search types, reports, case management, notifications, channels, and administrative functions for managing content, storage, archives, search filters, saved searches, search configuration, log retrieval and license information.
- **SmartConnectors** -- SmartConnectors are software components that forward security events from a wide variety of devices and security event sources to ESM. SmartConnectors are not bundled with ESM and are installed separately.

Below is a diagram of how these components can be deployed in a network:



ESM Components and Distributed Correlation

Distributed correlation allows you to use distributed resources as services to run on one or several systems (nodes) in a software cluster that you install, configure, and manage. A distributed correlation deployment includes the persistor, repository, correlators, aggregators, message bus data, message bus control, and distributed cache. Ideally, the correlators and aggregators in the cluster will keep up with event flow on your system. As needed, you can add more correlators and aggregators through configuration, as described in the Administrator's Guide.

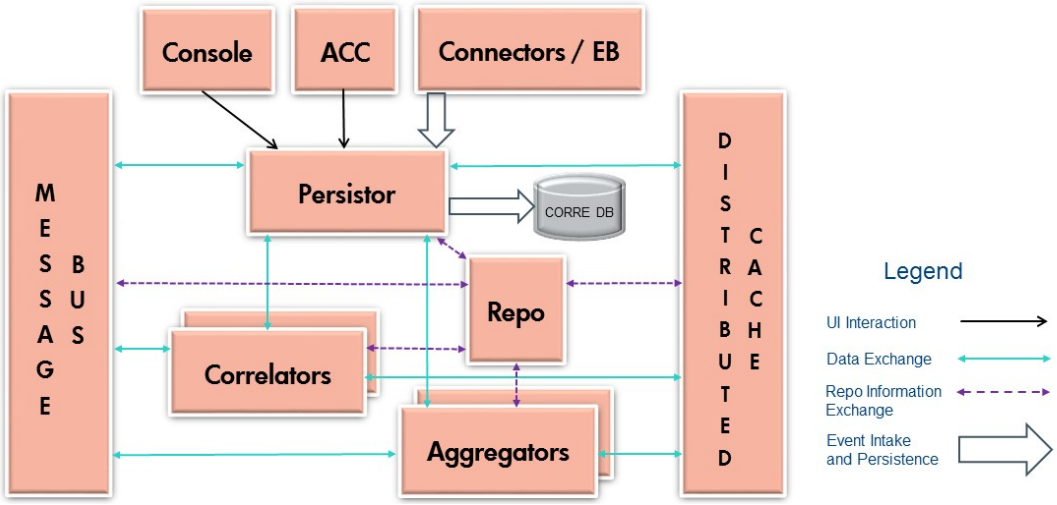
You must balance system resources as you add these components (CPU and memory). You will want to be somewhat generous in your cluster planning, and add more correlators and aggregators than you think you need. Distributed correlation is most effective if configured over multiple physical systems to ensure the fault tolerance benefit of the distributed correlation cluster deployment is fully realized. The fault tolerance aspect of the distributed correlation cluster, as described in "Distributed Correlation Concepts" in ESM 101.

Distributed correlation has components that are used in the context of cluster nodes:

- **Persistor:** Persists to disk the information that needs to be retained, retrieved, or shared. There is a single persistor in the distributed correlation cluster. The persistor consists of multiple entities, including the Manager, Logger, and the CORR-Engine database, among others. When you configure a distributed correlation cluster, the persistor is on the first node you configure during installation.
- **Correlators:** Each correlator in the cluster is a single process; there can be multiple correlators on each node in the cluster.

- **Aggregators:** Each aggregator in the cluster is a single process; there can be multiple aggregators on each node in the cluster.
- **Message Bus Control and Message Bus Data:** Handles the messaging among the cluster components.
- **Repository (Repo):** Contains the state of each member of the cluster among all of the nodes.
- **Distributed Cache:** Manages the short-term storage of data needed for cluster operation.

Here is a conceptual view of the cluster services and their interactions with each other and ESM:



ESM Communication Overview

The ArcSight Console, Manager, and SmartConnectors communicate using HTTPS (HyperText Transfer Protocol Secure). The HTTPS protocol provides for data encryption, data integrity verification, and authentication for both server and client.

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

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

Choosing between FIPS Mode or Default Mode

ESM supports the Federal Information Processing Standard (FIPS) 140-2 and Suite B. FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to

accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet FIPS 140-2 standards.

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

Note: FIPS 140-2 is the default selection.

Regardless of the mode you select, ensure that ESM and connectors use the same mode.

- Default mode (standard cryptography)
- FIPS 140-2 mode
- FIPS with Suite B mode (128 bits or 192 bits)

FIPS Encryption Cipher Suites

A cipher suite is a set of authentication, encryption, and data integrity algorithms used for securely exchanging data between an SSL server and a client. Depending on FIPS mode settings, some of the following specific cipher suites are automatically enabled for ESM and its clients.

Note: SSL is not supported in any mode. TLS is supported for all modes. For TLS version support see TLS Support.

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

Mode	Default cipher suites	Keystore/ truststore
Default mode	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256	Keypair and certificates stored in keystore and cacerts, and truststore in JKS format
FIPS 140-2 mode	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256	Keypair and certificates stored in keystore

Mode	Default cipher suites	Keystore/ truststore
FIPS with Suite B mode	• In 192-bit mode, the following 192-bit cipher suites are supported: ◦ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • In 128-bit mode, the following 128-bit cipher suites are supported: ◦ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◦ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Keypair and certificates stored in keystore

Using PKCS#11

ESM supports the use of a PKCS#11 token such as 90Meter or the Common Access Card (CAC) (which is used for identity verification and access control) to log into the Console. PKCS#11 is Public-Key Cryptography Standard (PKCS), published by RSA Laboratories which describes it as "a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards."

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

Effect on Communication When Components Fail

If any 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 is 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.

Directory Structure for ESM Installation

By default, ESM 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 for the Manager.

Port	Directory
ESM bin	`/opt/arcsight/manager/bin`
Properties files	`/opt/arcsight/manager/config`
Log files	`/opt/arcsight/var/logs`

References to ARCSIGHT_HOME

`<ARCSIGHT_HOME>` in the paths represents:

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

Specifying a Global Event ID Generator ID

Global event IDs uniquely identify events across the ArcSight product suite so that you can determine the origin of events that appear in multiple components. Although ESM mainly consumes events from components such as connectors and Transformation Hub, it also generates monitoring, correlation, audit, and other internal events that require a unique event ID. The ArcSight administrator must specify a global event ID generator ID that is unique and does not overlap with the global event ID generator IDs for other ArcSight products.

Note: When you specify the global event ID generator ID for ESM, it is important to verify that this ID does not conflict with the global event ID generator ID for other ArcSight components in your environment.

The global event ID generator ID will be used to generate global event IDs for the events that are generated within the ESM installation.

During installation, you must specify a global event ID generator ID that is an integer between 0 and 16384 (0 and 16384 are not valid IDs). When you assign a global event ID generator ID to an ArcSight component, it should remain the same throughout the lifetime of the component. Should it become necessary to change the generator ID, do not attempt to change it without contacting Technical Support.

Note: If you are installing in a distributed correlation environment, you only need to specify a global event ID generator ID on the persistor node.

If you specified a valid global event ID generator ID but for some reason ESM failed to store the ID, the installation proceeds but the ArcSight Manager will not start. This situation is not expected. In the event that this situation does occur, complete the following steps to resolve the issue:

1. Shut down the ArcSight Manager.
2. As user `arcsight`, run the following script:

   ```
   ./arcsight setgeidgenid <Global_Event__ID_Generator_ID>
   ```

   where `Global_Event_ID_Generator_ID` is an integer between 0 and 16384 (0 and 16384 are not valid)

   Note: In a distributed correlation environment, only run the script on the persistor node.
3. Restart the ArcSight Manager.

After you complete the installation, you can view the resources that are related to the global event ID by searching for the term "GEID" from the **Resources** search field in the ArcSight Console.

Understanding Exceptions to CIS Benchmarks and DISA Security Technical Implementation Guides

The section describes the areas in which ESM does not comply with Center for Internet Security (CIS) benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

Note: The information is specific to RHEL 7.7.

ESM installation does not comply with CIS benchmark 1.1.2, which states that `/tmp` should be a separate partition with the `noexec` mount option. This means that you cannot run a program underneath `/tmp`.

As a workaround, create the directory `<tmpdir>` as user `arcsight` and add the following lines to `/home/arcsight/.bashrc`:

```
export IATEMPDIR=<tmpdir>
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=<tmpdir>
```

```
export _JAVA_OPTIONS=-Djava.io.tmpdir=<tmpdir>
```

Before you run the installation, log out and then log in.

Micro Focus recommends using `/home/arcsight/tmp` for `<tmpdir>`, but you can use an alternate choice as appropriate for your environment.

Create a directory named "custom" in the extracted installation directory and ensure that the unzip rpm is installed on the operating system.

Chapter 2: Installing on an Appliance

This section applies to users who have purchased ESM on an appliance. For instructions about how to install ESM on your own hardware, go to Installing Software ESM.

Read the Release Notes before you begin.

Note: The operating system image provided on a G10 appliance does not include X Window. Since the X Window system is not present on ESM on an appliance, the installation and configuration of ESM on an appliance is performed using the command line. No GUI wizard is available for installation and configuration of ESM on an appliance.

There are no software preparations necessary on the appliance and no opportunity to make any preparatory adjustments before the First Boot Wizard starts.

Starting the Appliance for the First Time

When you power on the appliance, the Operating System First Boot Wizard (FBW) starts automatically. Ensure that Port 1 (the bottom left port) is connected to the network. The FBW offers three choices of networking types:

- IPv4
- IPv6
- Both IPv4 and IPv6 (dual stack)

Starting the Appliance for the First Time - IPv4

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

1. At appliance login, log in as user `root`, using the password `arcsight`.
2. Set a new password for user `root`.
3. Set a new password for user `arcsight`.
4. Set the appliance hostname.
5. Specify 1 for IPv4.
6. Specify the appliance IP address.
7. Specify the netmask.
8. Specify the default gateway.

9. Specify the primary DNS IP Address.
10. Specify the secondary DNS IP Address (optional).
11. Specify the DNS Search Domains.
12. Specify the time zone. You can start to type and press Tab and the system will attempt to auto-fill the time zone. For example you can type A, Tab and it fills in "America_". Press the Tab key twice for a list of time zone entries that starts with "America_".
13. Enter the Date.
    The date and time are optional. If you specify an NTP server, it overrides these date/time values. If there is no NTP server, these date/time values reset the appliance system clock and if you leave them blank, the system clock determines the date time.
14. Enter the Time.
15. Specify the NTP servers. List one NTP server per line. You can use IP addresses or host names. Using an NTP server is recommended.

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

If you accept the specifications, type **y** and press **Enter** to end the installation session and automatically start the Configuration Wizard.

License file: Once the IP address is defined you can log in to the appliance from the machine where you downloaded the license file and copy it to the appliance. The Configuration Wizard segment, which is next, asks you to specify the location of the license file on the appliance.

Starting the Appliance for the First Time - IPv6

For IPV6, you can specify Static or Auto Config Networking setups.

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

IPv6 Static Networking Setup

1. At appliance login, log in as user `root`, using the password `arcsight`.
2. Set a new password for user `root`.
3. Set a new password for user `arcsight`.
4. Set the appliance host name.
5. Specify 2 for IPv6.
6. Specify 1 for a static IPv6 networking setup (in which you will provide the IP address).
7. Specify the appliance IP address.

8. Specify the default gateway.
9. Specify the primary DNS IP Address.
10. Specify the secondary DNS IP Address (optional).
11. Specify the DNS Search Domains.
12. Specify the time zone. You can start to type and press Tab and the system will attempt to auto-fill the time zone. For example you can type A, Tab and it fills in "America_". Press the Tab key twice for a list of time zone entries that starts with "America_".
13. Enter the Date.
    The date and time are optional. If you specify an NTP server, it overrides these date/time values. If there is no NTP server, these date/time values reset the appliance system clock and if you leave them blank, the system clock determines the date time.
14. Enter the Time.
15. Specify the NTP servers. List one NTP server per line. You can use IP addresses or host names. Using an NTP server is recommended.

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

If you accept the specifications, type **y** and press **Enter** to end the installation session and automatically start the Configuration Wizard.

IPv6 Auto Config Networking Setup

1. At appliance login, log in as user `root`, using the password `arcsight`.
2. Set a new password for user `root`.
3. Set a new password for user `arcsight`.
4. Set the appliance host name.
5. Specify **2** for IPv6.
6. Specify **2** for an Auto Config IPv6 networking setup, which uses Stateless Address Auto Configuration (SLAAC). Specify the primary DNS IP address and, optionally, the secondary DNS IP address. The IP address and gateway address are automatically detected and assigned through the DNS.
7. Specify the time zone. You can start to type and press Tab and the system will attempt to auto-fill the time zone. For example you can type A, Tab and it fills in "America_". Press the Tab key twice for a list of time zone entries that starts with "America_".
8. Enter the Date.
   The date and time are optional. If you specify an NTP server, it overrides these date/time values. If there is no NTP server, these date/time values reset the appliance system clock and if you leave them blank, the system clock determines the date time.

9. Enter the Time.
10. Specify the NTP servers. List one NTP server per line. You can use IP addresses or host names. Using an NTP server is recommended.

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

If you accept the specifications, type **y** and press **Enter** to end the installation session and automatically start the Configuration Wizard.

License file: Once the IP address is defined you can log in to the appliance from the machine where you downloaded the license file and copy it to the appliance. The Configuration Wizard segment, which is next, asks you to specify the location of the license file on the appliance.

Starting the Appliance for the First Time - Dual Stack

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

1. At appliance login, log in as user `root`, using the password `arcsight`.
2. Set a new password for user `root`.
3. Set a new password for user `arcsight`.
4. Set the appliance host name.
5. Specify **3** for both IPv4 and IPv6.
6. Complete the choices for the IPv4 networking setup per the steps in Starting the Appliance for the First Time - IPv4.
7. Complete the choices for the IPv6 networking setup per the steps in Starting the Appliance for the First Time - IPv6.

When you are done, the FBW provides a list of what you have specified for both IPv4 and IPv6, for your review. If you choose `No`, it starts over.

If you accept the specifications for both IPv4 and IPv6, type **y** and press **Enter** to end the installation session and automatically start the Configuration Wizard.

License file: Once the IP address is defined you can log in to the appliance from the machine where you downloaded the license file and copy it to the appliance. The Configuration Wizard segment, which is next, asks you to specify the location of the license file on the appliance.

Installing on an Appliance Using the Configuration Wizard

When installing on an appliance, the configuration wizard starts automatically. You do not need to manually enter a command to start the appliance.

You can rerun the wizard manually only if you exit it at any point **before** you reach the About to Configure screen. For more information about running the wizard manually, see Re-running the ESM Configuration Wizard.

Note: Distributed correlation mode is not available on an appliance.

When you run the `managersetup` command on the appliance, you will receive the following messages:

```
Wizard could not connect to an X11 display.
Please set the DISPLAY variable to start the wizard in UI mode.
Falling back to console mode.
```

You can ignore these messages.

Specifying the ArcSight Manager Host Name

During the installation, the wizard prompts you to specify the ArcSight Manager host name. Keep the following points in mind when specifying the host name:

- The Manager host name is used to generate a self-signed certificate. The Common Name (CN) in the certificate is the host name that you specify when prompted.
- The Manager host name is the IP address (for IPv4 only) or the fully-qualified domain name of the machine where the Manager is installed. All clients (for example, the ArcSight Console) use this name to connect to the Manager. For flexibility, Micro Focus recommends using a fully-qualified domain name instead of an IP address.
- If you are installing on a dual-stack machine, the wizard prompts you to select the preferred IP protocol. Your selection controls the following:
  - The IP address that third-party software uses if a host name is given. For example, the email server in Manager Setup.
  - The IP address that is used on the peering page if a host name is given.
  - Whether an IPv4 or an IPv6 address is used for the manager asset.
- The Manager might have more than one host name, and the default name might not be the

same as the name returned by the `hostname` command. If you are using the High Availability Module, use the service host name that is common to both servers (primary and secondary) as the Manager host name. Otherwise, choose the name that you expect to work and that is convenient for configuring connectors, consoles, and other clients.

Micro Focus recommends using the fully-qualified domain name.

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

To install ESM on an appliance:

1. Ensure that the license file is accessible and type **yes**.
2. Select the language for interface displays.
3. Specify **0** to install ESM in compact mode.

   Note: The other option, **Distributed Mode**, is not available on an appliance.

4. For **CORR-Engine Password**, complete the following:
   a. Press **Enter** to continue with obfuscated passwords or type **no** to display passwords.
   b. Specify a password for the CORR-Engine and verify the password.

      For information about password restrictions, see the Administrator's Guide.
5. For **CORR-Engine Configuration**, specify the following information:
   a. **System Storage Size** - amount of storage space to set aside for storing resources
   b. **Event Storage Size** - amount of storage space to set aside for storing events
   c. **Online Event Archive Size** - maximum number of gigabytes of disk space for event archives
   d. **Retention Period** - amount of time that you want to retain events before they are purged from the system
6. For **Notification Emails**, specify the following information:
   a. Specify an email account to receive email notifications if the Manager becomes unavailable or encounters some other problem.

      You can use the Manager Configuration Wizard to specify more email addresses. For more information, see the Administrator's Guide.
   b. Specify an email address for the sender of notification emails.

   Notification emails will be sent in the following situations:

   - The subsystem status changes. The email includes information about the the change and who made it.

- The report is successfully archived.
- The account password is reset.
- The archive report generation fails.
- A destination receives too many notifications.
- The event archive location reaches the cap space. The notification requests that you free up space by moving the event archives to another location.
- The user elects to email the ArcSight Console settings.
- The user sends a partition archival command.
- An archive fails because there is not enough space.
- The connection to the database fails.

7. Provide the path and file name of the license file that you downloaded.
8. Select whether to install in default mode or FIPS mode.

Note: FIPS 140-2 mode is the default selection.

Regardless of the mode you select, ensure that ESM and connectors use the same mode.

Caution:

- If you choose to install in FIPS mode, you must also install the ArcSight Console in FIPS mode. For more information, see Installing the ArcSight Console in FIPS Mode.
- After you configure ESM in FIPS mode, you cannot convert it to default mode without reinstalling it.
- Converting from default mode installation to FIPS-140-2 mode is supported. For more information, see the Administrator's Guide.
- By default, ESM uses a self-signed certificate. To use a CA-signed certificate, you must import the CA-signed certificate manually **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.

9. If you selected to install in FIPS mode, select the cipher suite.

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

a. Host name

b. Credentials for the admin user

For considerations that apply to the Manager host name, see Specifying the ArcSight Manager Host Name.

By default, the Manager uses a self-signed certificate. To use a CA-signed certificate, you must import the CA-signed certificate manually **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.

11. Specify the global event ID generator ID that will be used to generate global event IDs.

    You must specify an integer between 0 and 16384 (0 and 16384 are not valid). For more information, see Specifying a Global Event ID Generator ID.

12. If Transformation Hub is part of your ESM implementation, select whether to set up a connection to it.

    For more information, see the applicable topic:

    - Configuring Transformation Hub Access - Non-FIPS Mode
    - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode
    - Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)
    - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

    Note: If ESM will connect to Kafka using SASL/PLAIN authentication, skip this step and use `managersetup` to configure the connection after you complete the initial configuration. For more information, see Completing Post-Installation Tasks.

    If you select to set up a connection, provide the following information:

    a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

       Note: You must specify the host name and *not* the IP address.

       Transformation Hub can only accept IPv4 connections from ESM.

    b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

       For more information, see the Administrator's Guide for the ArcSight Platform.

> **Note:** You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2).

c. Import the Transformation Hub root certificate to ESM's client truststore.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Copy the Transformation Hub root certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` on the Transformation Hub server to a local folder on the ESM server. After you provide the path to the certificate, the wizard imports the Transformation Hub root certificate into ESM's client truststore and validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

13. Select whether to integrate Recon.

    If you select to integrate, specify the **Search URL** for the Recon deployment.

    > **Note:** ArcSight ESM version 7.5 requires Recon 1.1.0.

14. Select whether to integrate with the ServiceNow® IT Service Management (ITSM) application.

    If you select **Yes**, specify the mandatory **ServiceNow URL** and the optional **ServiceNow Proxy URL**.

    For information about completing the configuration, see Configuring Integration with ServiceNow®.

15. If you are not licensed to use optional packages, press **Enter** to advance to the next screen. Otherwise, select the optional packages that you are licensed to use. In addition to these optional packages, default standard content packages are installed automatically on the ArcSight Manager. These default packages provide essential system health and status operations, and you can use them immediately to monitor and protect your network.

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

16. Select to continue with the installation. You will receive a message when the installation is complete.

17. Log in as user root and run the following script to set up and start the required services:

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

18. Check the location and size of your storage volumes and use ArcSight Command Center to make any necessary changes. For more information, see the Command Center User's Guide.

Keep These TCP Ports Open

On an appliance, these ports are already open.

Ports for external incoming connections:

8443/tcp
22/tcp (ssh)

TCP ports used internally for inter-component communication:

1976, 28001, 2812, 3306, 5555, 6005, 6009, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8765, 8766, 8881, 8808, 8880, 8888, 8889, 9095, 9090, 9123, 9124, 9999, 45450

Enable Peering

This topic is for appliance installation using an ESM license that includes peering.

By default appliances ship with port 9000 disabled. Peering requires this port. For peering to work on an appliance, enable port 9000 using the following commands:

```
[root@rhel7 ~]# firewall-cmd --zone=public --add-port=9000/tcp --permanent
```

```
[root@rhel7 ~]# firewall-cmd --reload
```

Use this command to check that port 9000 is enabled:

```
[root@rhel7 ~]# iptables-save | grep 9000
```

You should get response similar to this:

```
 -A IN_public_allow -p tcp -m tcp --dport 9000 -m conntrack --ctstate NEW -j
ACCEPT
```

Note that peering works between ESM Managers that use the same IP version. However, if an ESM Manager is on a dual-stack machine, see the Command Center User's Guide.

Running ESM on an Encrypted Appliance

ESM can be run on encrypted hardware to help you to meet compliance regulations and privacy challenges by securing your sensitive data at rest. This includes systems using the HighAvailability Module; the HA functionality is exactly the same.

You can encrypt your G10 ESM Express appliance (such as B7600 or E7600) by using Secure Encryption, available from the Server Management Software > Secure Encryption web page. For instructions, refer to the *Secure Encryption Installation and User Guide*, available in PDF and CHM formats through the Technical Support > Manuals link on that page.

G10 Appliances are encryption-capable. They come pre-installed with everything necessary for you to encrypt them using Secure Encryption. You can encrypt your hardware before or after ESM is installed. If HA is already installed, encrypt the secondary first, so you only have to failover once.

The length of time encryption takes depends on the amount of data on the server being encrypted. In our testing, a Gen 9 appliance with 7.5 TB of stored data took about 72 hours to encrypt. You can continue using ESM while the encryption runs. You may notice some performance degradation after encrypting your ESM appliance.

Caution: After encryption, you cannot restore your ESM to its previously unencrypted state.

Configuring the Appliance for Out-of-Band Remote Access

Configure the appliance for out-of-band remote access so that Customer Support can access and troubleshoot the appliance if it becomes unresponsive. All appliance models are equipped with the Integrated Lights-Out (iLO) advanced remote management card.

Chapter 3: Installing Software ESM

Micro Focus recommends that you read the *ESM* Release Notes before you begin installing ESM.

If you are installing ESM Express, which is on an appliance, see Installing on an Appliance.

If you are going to use the Active Passive High Availability (APHA) Module with ESM and this is a new ESM installation, install the HA Module first. For more information, see the Active Passive High Availability Module User's Guide. Note that you must install ESM after APHA has completed disk synchronization. Attempting to install ESM while APHA synchronization is in process can cause the ESM installation to fail.

ESM is sensitive to the operating system and version. To ensure proper operation, this installer only allows installation on the specific operating systems and versions listed in the *Technical Requirements* on the ESM documentation page.

Securing Your ESM System

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

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:

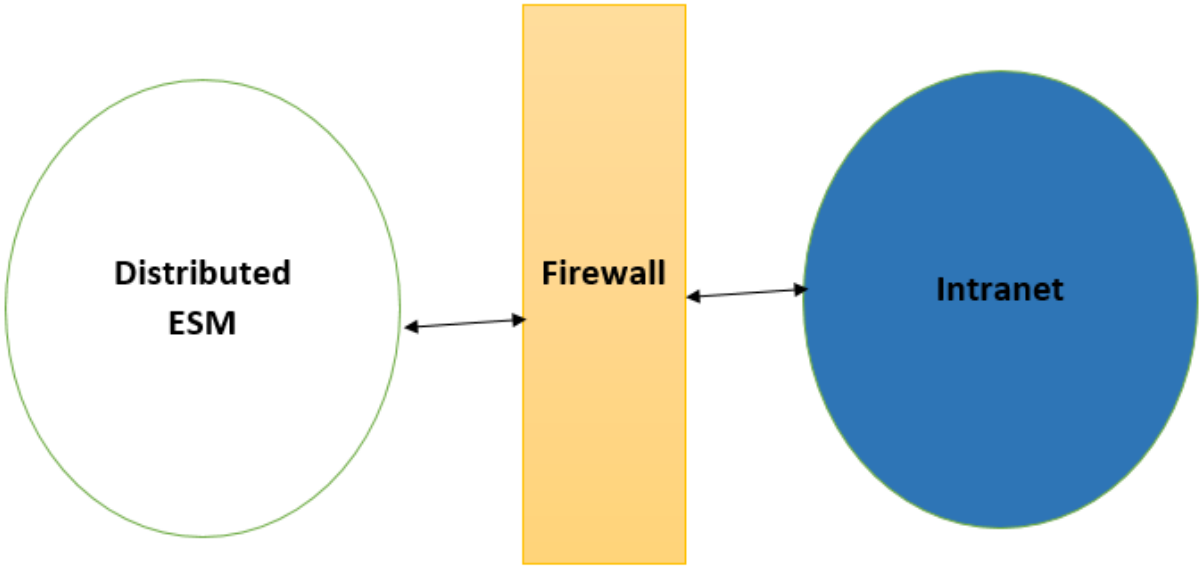
Note: `<ARCSIGHT_HOME>` is the root directory for a component. For example for the Manager component, `<ARCSIGHT_HOME>` is: `/opt/arcsight/manager`.

- `<ARCSIGHT_HOME>/config/jetty/keystore` (to prevent the ArcSight Manager private key from being stolen)
- `<ARCSIGHT_HOME>/config/jetty/truststore` (with SSL client authentication only, to prevent injection of new trusted CAs)
- `<ARCSIGHT_HOME>/config/server.properties` (has database passwords)
- `<ARCSIGHT_HOME>/config/esm.properties` (has cluster configuration properties and SSL properties common to persistor, correlator, and aggregator services on the node)

  This properties file is present on each node in a distributed correlation cluster.

- `<ARCSIGHT_HOME>/config/jaas.config` (with RADIUS or SecurID enabled only, has shared node secret)
- `<ARCSIGHT_HOME>/config/client.properties` (with 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)

If you are installing ESM on your own hardware (as opposed to an appliance), use a firewall. Micro Focus recommends a host-based firewall for compact mode. For distributed mode, you will need a firewall between all of the hosts in the cluster and the rest of the intranet. Servers in a distributed cluster should not have host-based firewalls, and there should not be firewalls between the servers in a cluster. For example:



On the firewall, block everything except the following ports. Ensure that you restrict the remote IP addresses that might connect to those that actually need to talk.

Port	Flow	Description
22/TCP	Inbound	SSH log in
53/UDP	Inbound/Outbound	DNS requests and responses

Port	Flow	Description
8443/TCP	Inbound	SmartConnectors and Consoles **Note:** This port is only necessary in compact mode or for communication to the persistor node.
25/TCP	Outbound	SMTP to mail server **Note:** ESM only requires email in compact mode or on the persistor node.
110/TCP	Outbound	POP3 to mail server **Note:** ESM only requires email in compact mode or on the persistor node.
143/TCP	Outbound	IMAP to mail server **Note:** ESM only requires email in compact mode or on the persistor node.
1645/UDP	Inbound/Outbound	RADIUS **Note:** This port is only necessary in compact mode or for communication to the persistor node.
1812/UDP	Inbound/Outbound	RADIUS, if applicable **Note:** This port is only necessary in compact mode or for communication to the persistor node.
389/TCP	Outbound	LDAP to LDAP server, if applicable
636/TCP	Outbound	LDAP over SSL to LDAP server, if applicable
9000/TCP	Inbound/Outbound	Logger peering, if applicable **Note:** This port is only necessary in compact mode or for communication to the persistor node.

Applies to IPv4 only:

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

```
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.
- 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. (Being "registered" does not mean you can then remove them.)

The format for specifying subnets is quite flexible, as shown in the following example:

```
xmlrpc.accept.ips=192.0.2.0 192.0.2.5
agents.accept.ips=10.*.*.*,192.0.0.0-192.0.255.255
```

Built-In Security

ESM 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 automated 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.

By default, the minimum length for passwords is six characters and the maximum length is 20 characters. For information about password restrictions, see the Administrator's Guide.

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

Complete the following items to ensure operating system security:

- Before you install ESM, install an entropy generator (normally provided by your operating system vendor) such `rng-tools` or `haveged`. ESM requires high levels of operating system entropy for secure cryptography.
- On Linux, set up a boot loader password to prevent unauthorized people from booting into single user mode (see the iLO or GRUB documentation for details).
- On Linux, disable reboot caused by Ctrl-Alt-Delete:
  - On versions using "upstart" such as CentOS/RHEL 6, run the following command as `root`:

    ```
    echo "exec /bin/true" > /etc/init/control-alt-delete.override ; initctl
    reload-configuration control-alt-delete
    ```

  - On versions using "systemd" such as CentOS/RHEL 7, run the following command as `root`:

    ```
    systemctl mask ctrl-alt-del.target
    ```

- 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 more difficult to perform.

General Guidelines and Policies about Security

Educate system users about “social engineering” tricks used to discover user account information. No employee of Micro Focus will ever request a user’s password. When Micro

Focus 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 Micro Focus team to work effectively.

Educate users to use secure means of communication (such as SSL to upload or PGP for e-mail) when transferring configuration information or log files to Micro Focus.

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. See the Administrator's Guide or contact Customer Support 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 about password restrictions, see the Administrator's Guide.

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 (with 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.

Preparing to Install

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

System Requirements

The hardware requirements for ESM 7.5 are as follows:

	Minimum	Mid-Range	High Performance
Processors	8 cores (16 preferred)	32 cores	40 cores
Memory	48 GB RAM (64 preferred)	192 GB RAM	512 GB RAM
Hard Disk	Six 600 GB disks (1.5 TB) (RAID 10) 10,000 RPM	20 1 TB disks (10 TB) (RAID 10) 15,000 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 Threat Detector (formerly known as 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 Sales or Field Representative.

If you anticipate that you will have large lists, ensure that your system meets the Mid-Range requirements or better.

Manager Host Name Resolution

Before ESM installation, make sure that the host machine's hostname is resolvable, otherwise, Manager setup will not complete successfully. Use `ping` to verify the hostname, and fix any issues to avoid errors during Manager setup.

Login Banners

Login banners might interfere with a distributed cluster installation. The following types of login banners are safe to use:

- "Message of the day" (`/etc/motd`) and other banners that do not appear when running a remote command
- SSH login banners that you configure in `/etc/ssh/sshd_config`

Other login banners (for example, echo statements in ~/.bashrc) might cause ESM to fail during or after a distributed cluster installation.

Mapping 127.0.0.1 to localhost

Make sure that the IP address 127.0.0.1 is resolved to `localhost` in the `/etc/hosts` file, otherwise, the ESM installation will fail. This applies to IPv4 and IPv6 systems.

Monitor Requirement

For displaying the ArcSight Command Center, use a monitor that has a width of at least 1450 pixels. This is the minimum width needed to display all of the top-menu items without cutting any of them off. This minimum width also applies on a larger monitor when reducing the size of the browser window.

Supported Platforms

ESM 7.5 is supported on 64-bit Red Hat Enterprise Linux (RHEL), CentOS, and SUSE Linux Enterprise Server (SLES). For supported versions, see the *Technical Requirements* on the ESM documentation page. Install the operating system using at least the **Web Server** option with added **Compatibility Libraries** and **Development Tools**. ESM is sensitive to the operating system and version.

Keep the following points in mind regarding the operating system:

- To install ESM in GUI mode, install the X Windows system package. X Windows is optional. For RHEL or CentOS, install `xorg-x11-server-utils-7.5-13.el6.x86_64` or a later version. If you do not use X Windows, you can install ESM in console mode.
- The XFS and EXT4 file system formats are supported during installation.
- ESM configures itself to the file system upon which you install it. You cannot change the file system type after installation, even during an upgrade.

Required RPM Packages

The following RPM packages are required for the ESM installation:

- `zip`
- `unzip`
- `libaio`

Ensure zip is installed

Run the following command to verify that the required `zip` RPM package is installed:

```
rpm -qa zip
```

If the package is not installed, install it using the following command for your platform:

- On RHEL and CentOS, run the following command:

  ```
  yum install zip
  ```

- On SLES, run the following command:

  ```
  zypper install zip
  ```

Ensure unzip is installed

Run the following command to verify that the required `unzip` RPM package is installed:

```
rpm -qa | grep unzip
```

If the package is not installed, install it using the following commands for your platform:

- On RHEL and CentOS, run the following command:

  ```
  yum install unzip
  ```

- On SLES, run the following command:

  ```
  zypper install unzip
  ```

Ensure libaio is installed

Run the following command to verify that the required `libaio` RPM package is installed:

```
rpm -qa | grep libaio
```

The output should be similar to the following:

```
libaio-0.3.109-13.el7.x86_64
```

If the package is not installed, install it using the following command for your platform:

- On RHEL and CentOS, run the following command:

  ```
  yum install libaio
  ```

- On SLES, run the following command:

  ```
  zypper install libaio1
  ```

Download the Installation Package

The ESM7.5 installation package is available for download at: https://softwaresupport.softwaregrp.com/. Download the `ArcSightESMSuite-7.5.0.xxxx.0.tar` file and copy it to the system where you will be installing ESM. The xxxx in the file name stands for the build number.

After you download the software, contact support to verify that the signed software you received is indeed from Micro Focus and has not been manipulated by a third party.

After you download the .tar file from the software download site, initiate license procurement by following the instructions in the Electronic Delivery Receipt you receive in an email after placing the order.

Preparing the System

1. As user `root`, run the following command to untar the installation package:

   ```
   tar xvf ArcSightESMSuite-7.5.0.xxxx.0.tar
   ```

   ESM places the `prepare_system.sh` script in a `Tools` subdirectory in the location where you untarred the file.
2. Run `prepare_system.sh`.
3. Change ownership of all the files and folders that were extracted from the tar file to user `arcsight`.

4. Reboot the system.
5. To verify that the script ran correctly, as user `root`, run:

   ```
   ulimit -a
   ```

   Check for the following lines:
   ```
   open files 65536
   max user processes 10240
   ```

Keep these TCP Ports Open

Before you install software ESM, open the ports that are listed in this section if they are not already open. Ensure that no other processes are using these ports.

Open the following ports for external incoming connections:

8443/TCP - SmartConnectors and consoles
9000/TCP - Peering
5404/UDP - High Availability module
5405/UDP - High Availability module
7789/TCP - High Availability module
22/TCP - SSH login

Open the following TCP ports for inter-component communication:

1976, 2812, 3306, 5555, 6005, 6009, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8765, 8766, 8808, 8880, 8881, 8888, 8889, 9000, 9090, 9095, 9123, 9124, 9999, 28001, 45450

Some ports are used in a distributed correlation environment. The information repository uses ports 3179, 3180, 3181, and 3182. Also, there are port ranges reserved for use by cluster services. Other processes must not use ports in these reserved ranges. For more information about reserved port ranges, see the Administrator's Guide.

Installing the Time Zone Update Package

ESM uses the time zone update package to automatically handle changes in time zone or changes between standard and daylight savings time. During installation, ESM verifies whether the appropriate operating system time zone update package is installed. If it is not, you have the option to exit the installation program and install the latest package or continue the ESM installation and install the time zone update package later. Micro Focus recommends installing the time zone update package when prompted.

The package to use depends on your operating system version:

For this operating system:	Use this package or later:
RHEL or CentOS 8.2 or 8.1	`tzdata-2020f-1.el8.noarch.rpm`
RHEL or CentOS 7.9, 7.8, or 7.7	`tzdata-2020f-1.el7.noarch.rpm`
SLES 15 Service Pack 1	`timezone-2020f-3.41.2.x86_64.rpm`
SLES 12 Service Pack 5	`timezone-2020f-74.46.1.x86_64.rpm`

To install the time zone update package before installation:

1. Unpack the package and upload it to your server (for example, to `/opt/work/<package name>`).
2. As user `root`, run the following command:

   ```
   rpm -Uvh /opt/work/<package name>
   ```

3. To check the time zone setting, run the following command:

   ```
   timedatectl
   ```

4. If the time zone is not correct or it is not the desired time zone, run the following command to specify another time zone:

   ```
   timedatectl set-timezone <time zone>
   ```

   For example:

   `timedatectl set-timezone America/Los_Angeles`

To install the time zone update package after you complete the ESM installation:

1. Use the procedure above to install the correct time zone update package.
2. As user `arcsight`, shut down all ArcSight services:

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

3. As user `arcsight`, run the following command (all on one line):

   ```
   /opt/arcsight/java/esm/current/jre/bin/java -jar
   /opt/arcsight/manager/lib/jre-tools/tzupdater/ziupdater-1.1.1.1.jar -V
   ```

4. As user `arcsight`, start all ArcSight services:

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

Set Directory Sizes

Make sure that the partition in which your `/tmp` directory resides has at least 6 GB of space.

Make sure that the partition in which your `/opt/arcsight` directory resides has at least 100 GB of space.

Sizing Guidelines for CORR-Engine

When installing ESM 7.5, 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 into consideration when changing storage sizes.

Note: Any events that are brought from an offline archive into the online archive count as part of the total 12 TB (or license determined) storage limit. You do not want the offline archives that you bring back online to encompass the entire storage limit. Use discretion when bringing offline archives online, and be sure to make them offline again when you are done working with them.

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

Event Storage - storage for events

Event Archive Size - archive of online events

	Recommended	Minimum	Maximum
System Storage Size	The default is about one sixth of Usable Space, from at least 3 GB up to a maximum of 1,500 GB. During installation, it is recommended that you accept the default.	3 GB	1,500 GB
Event Storage Size	Specify about two thirds of the Usable Space shown during installation.	10 GB	12 TB
Event Archive Size	You may specify the remaining space after the System and Event storage have been allocated.	1 GB	Limit is predicated on your file system size.

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

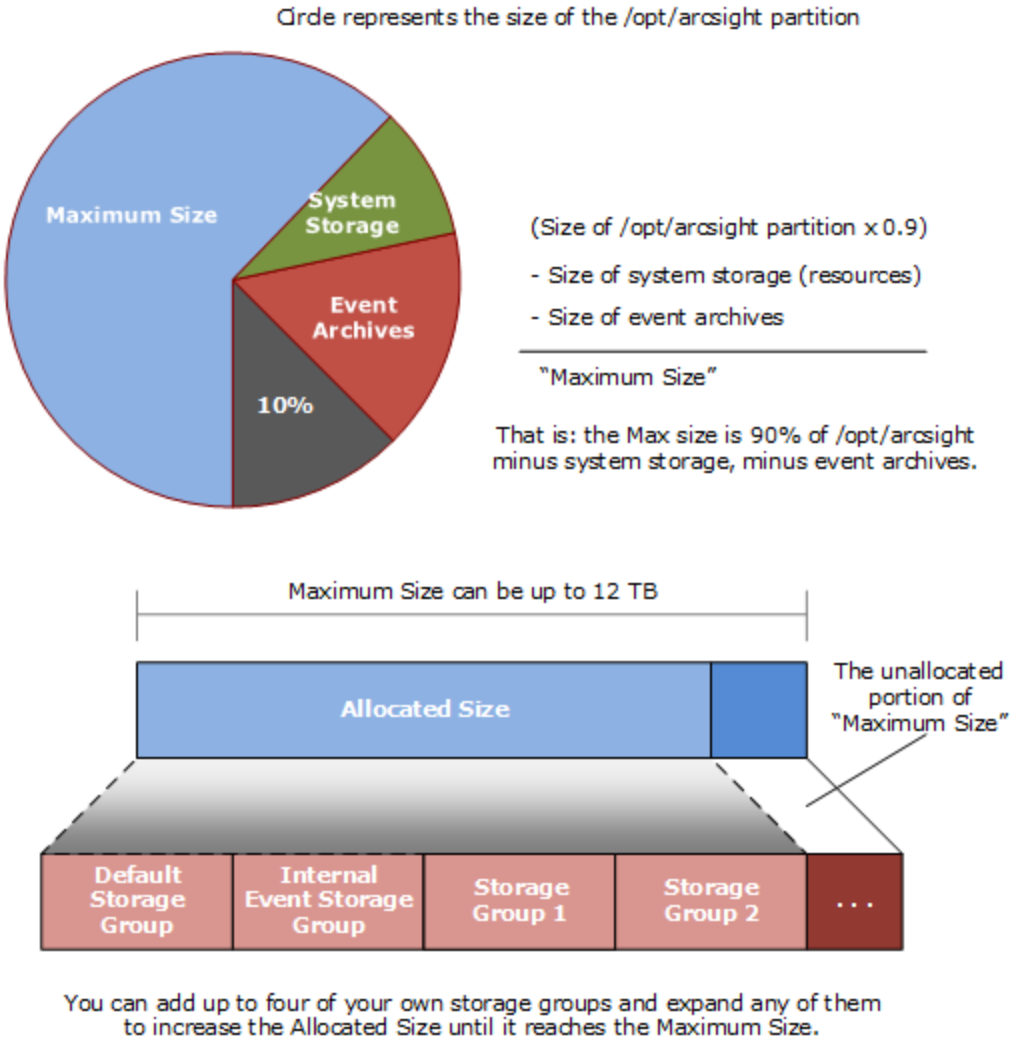
During installation, the system will show the size of the `/opt/arcsight` partition as Available Space, and the size of that partition less 10 percent reserved space designated as Usable Space. The maximum event storage volume size is calculated by the system using this formula: `Maximum Event Storage = /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. For more information, see the Command Center User's Guide.

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



Export Language UTF File

Run the following command:

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

where `[language]` is one of the following:
`en_US` (English)
`zh_CN` (Simplified Chinese)
`zh_TW` (Traditional Chinese)
`ja_JP` (Japanese)
`fr_FR` (French)
`ko_KR` (Korean)
`ru_RU` (Russian)

For example: `export LC_ALL=en_US.UTF-8`

Planning for a Distributed Correlation Cluster

This section describes items to consider before you install ESM in distributed correlation mode as described in Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard. A distributed correlation deployment includes the persistor, information repository, correlators, aggregators, message bus data, message bus control, and distributed cache. Ideally, the correlators and aggregators in the cluster will keep up with event flow on your system.

You must balance system resources as you add these components (CPU and memory). Be somewhat generous in your cluster planning and add more correlators and aggregators than you think you need. To achieve maximum fault tolerance, configure the cluster over multiple physical systems. For more information about distributed correlation and fault tolerance, see ESM 101.

Note: In the context of a distributed correlation implementation, ESM is the *entire cluster*. The individual cluster nodes are part of the fuller implementation, and do not function independently. Dedicate the systems that are the cluster nodes for cluster use only.

Converting Hierarchical Implementations to a Distributed Correlation Cluster

If you have been using a hierarchical implementation of ESM in order to achieve higher performance, consider implementing a distributed correlation cluster to increase EPS. You can convert your upgraded system to a cluster implementation, repurposing the systems that were part of your hierarchical implementation and adding more as needed. If you use a hierarchical implementation of ESM to gain benefits other than higher performance, such as combining feeds from various geographical areas, then a cluster implementation is not the favored solution.

Understanding Cluster Requirements

When planning your distributed correlation cluster, ensure that the cluster meets the following requirements:

- All nodes must be identical with regard to the following:
  - Operating system version
  - Time zone
  - FIPS mode (if FIPS mode is in use)
  - IP protocol (IPv4 or IPv6)

    Dual stack systems are supported, but all ESM IP addresses on all nodes must be either IPv4 or IPv6.
- Each server host name must resolve to an IP address for each cluster node. Otherwise, the installation will fail with an error message.

Note: If you expect heavy use (>30,000 EPS, large numbers of rules and data monitors, and large active lists and session lists), Micro Focus recommends 32 GB as the minimum heap memory size for the `manager` service on the persistor node.

Placing Information Repository Instances on a Separate Partition

In a distributed correlation environment, running an information repository instance on the disk partition that contains `/opt/arcsight` leads to performance problems. To avoid these problems, you must create `/var/opt/arcsight` (as a directory or a symbolic link to a directory) on all of the cluster nodes before you install ESM. During installation, the installation program places repository data in the partition that contains `/var/opt/arcsight` if it exists. Otherwise, it places repository data in the partition that contains `/opt/arcsight`.

The `/var/opt/arcsight` directory (or the directory that it points to) must meet the following requirements:

- `/var/opt/arcsight` must **not** be in the same partition that contains `/opt/arcsight`.
- The `arcsight` user must own the directory.
- The partition that contains `/var/opt/arcsight` must have at least 1 GB of free disk space.

Understanding Recommended Cluster Configurations

A node in an ESM cluster can be a physical server or a virtual machine, depending on your performance needs and resources. You can configure a cluster to run ESM services on multiple nodes. This section describes the recommended cluster configurations.

The number of correlators and aggregators you configure in your cluster will depend on the settings in your ESM implementation. For example, if you have complex filters and rule conditions, you might need more correlators. If you have a large number of data monitors or use complex join rules, you might need more aggregators. In general, Micro Focus recommends one correlator for each aggregator. Lags in the Cluster View dashboard in the ArcSight Command Center can indicate that you need more correlators or aggregators.

The total number of message bus control (`mbus_control`) instances must be either one or three for the cluster. Do not configure a message bus control instance on the persistor node.

Caution: If you plan to install the Active Passive High Availability (APHA) module on the persistor node, do not configure a message bus data instance on the persistor node. Otherwise, the cluster is likely to fail when ESM swaps the primary and secondary systems.

The total number of information repository (`repo`) instances must be either one or three for the cluster.

Note: Because having a `repo` instance on an APHA persistor node causes poor performance, Micro Focus does not recommend it. If you have an APHA persistor and at least four nodes (recommended), the installation program configures a `repo` instance on the persistor node, but later converts the cluster to have three `repo` instances, all on non-persistor nodes.

The total number of distributed cache (`dcache`) instances should be an odd number.

Micro Focus recommends starting with a four-node or five-node cluster, as these cluster sizes have been tested. You are not limited to five nodes and can add more nodes later if needed. For information about adding nodes after the initial installation, see the Administrator's Guide.

Small Configuration (Good)

The small configuration consists of four nodes, distributed as described below and with the recommended resources:

The persistor node has the following minimum hardware requirements:

- 192 GB RAM
- 8 TB disk
- 24 cores
- 10 Gbit network

The remaining nodes have the following minimum hardware requirements:

- 128 GB RAM
- 6 TB disk

- 24 cores
- 10 Gbit network

The nodes have the following software requirements:

- Node 1:
  - One persistor
  - One distributed cache
  - One information repository
- Node 2:
  - One correlator
  - One aggregator
  - One distributed cache
  - One message bus control
  - One message bus data
- Node 3:
  - One correlator
  - One aggregator
  - One message bus control
  - One message bus data
  - One information repository
- Node 4:
  - One correlator
  - One aggregator
  - One distributed cache
  - One message bus control
  - One message bus data
  - One information repository

Large Configuration (Best)

The large configuration consists of five nodes, distributed as described below and with the recommended resources:

All nodes have the following minimum hardware requirements:

- 256 GB RAM
- 8 TB disk

- 32 cores
- 10 Gbit network

The nodes have the following software requirements:

- Node 1:
  - One persistor
  - One distributed cache
  - One information repository
- Node 2:
  - One correlator
  - One aggregator
  - One distributed cache
  - One message bus control
  - One message bus data
- Node 3:
  - One correlator
  - One aggregator
  - One distributed cache
  - One message bus control
  - One message bus data
  - One information repository
- Node 4:
  - One correlator
  - One aggregator
  - One distributed cache
  - One message bus control
  - One message bus data
  - One information repository
- Node 5:
  - One distributed cache
  - One message bus data
  - One correlator
  - One aggregator

Choosing the Preferred IP Protocol

When you install ESM on the persistor node, you select whether IPv4 or IPv6 is the preferred protocol. When you select the preferred protocol, ensure that each host name for each host in the cluster resolves to an IP address of the protocol that you select on that host. For example, if the preferred protocol is IPv6 then each host name must resolve to an IPv6 address that is configured on that host.

Preparing for IPv6 Only Communication

If ESM will rely on IPv6 communication only, remove IPv4 interfaces. Micro Focus recommends keeping the 127.0.0.1 (localhost - le0) interface, but remove other IPv4 interfaces, especially virbr0 (typically IPv4 by default). In some cases, IPv4 interfaces cause the installation program to have problems resolving the host name of the server.

Starting the Installer

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

If not already granted, give the `ArcSightESMSuite.bin` file the execute permission:

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

Run the installation file as follows:

```
./ArcSightESMSuite.bin -i console
```

(or `./ArcSightESMSuite.bin`, for GUI mode, if you are using X Window.)

The installation begins.

Note:

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

The next topic picks up after the installer has started.

Running the Installation File

The following steps describe the ESM installer.

1. Read the **Introduction** message and press **Enter**.
2. On the **License Agreement** panel, press **Enter** to page through the agreement. In GUI mode, the "I accept the terms of the License Agreement" check box is disabled until you scroll to the bottom of the agreement text. If you accept the License Agreement, type **y** and press **Enter**.
3. Read the **Special Notice** and press **Enter**.
4. Under **Choose Link Folder**, enter the number for the location where you would like the installer to place the links for this installation and press **Enter**.
5. Review the **Pre-Installation Summary**. Press **Enter** to continue.

   Under **Installing** a progress bar appears.

The Suite Installer installs each component.

- In Console mode, after the components are installed it says **Installation Complete**. Press **Enter** to exit the installer. Go to the next topic, Starting the Configuration Wizard In Console Mode.
- In GUI mode, after the components are installed, the Configuration Wizard GUI opens automatically. Go to Installing Software ESM in Compact Mode Using the Configuration Wizard or Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard for details on configuring ESM.

> **Note:** In GUI mode, if you get a dialog box reporting an error or problem and the action button says **Quit**, use the **Quit** button. If you use the **X** in the upper right corner of the dialog, the process does not quit, but cannot complete successfully with the reported error.

Starting the Configuration Wizard In Console Mode

If you are installing software ESM in GUI mode or installing ESM Express, the configuration wizard starts automatically and you can skip this step during initial installation.

When installing software 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 start the configuration wizard manually by issuing the following command:

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

Installing Software ESM in Compact Mode Using the Configuration Wizard

This section describes installing ESM in compact mode. To install ESM in distributed correlation mode (using a cluster implementation) see Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard.

You can rerun the wizard manually only if you exit it at any point **before** you reach the About to Configure screen. For more information about running the wizard manually, see Re-running the ESM Configuration Wizard.

Specifying the ArcSight Manager Host Name

During the installation, the wizard prompts you to specify the ArcSight Manager host name. Keep the following points in mind when specifying the host name:

- The Manager host name is used to generate a self-signed certificate. The Common Name (CN) in the certificate is the host name that you specify when prompted.
- The Manager host name is the IP address (for IPv4 only) or the fully-qualified domain name of the machine where the Manager is installed. All clients (for example, the ArcSight Console) use this name to connect to the Manager. For flexibility, Micro Focus recommends using a fully-qualified domain name instead of an IP address.
- If you are installing on a dual-stack machine, the wizard prompts you to select the preferred IP protocol. Your selection controls the following:
  - The IP address that third-party software uses if a host name is given. For example, the email server in Manager Setup.
  - The IP address that is used on the peering page if a host name is given.
  - Whether an IPv4 or an IPv6 address is used for the manager asset.
- The Manager might have more than one host name, and the default name might not be the same as the name returned by the `hostname` command. If you are using the High Availability Module, use the service host name that is common to both servers (primary and secondary) as the Manager host name. Otherwise, choose the name that you expect to work and that is convenient for configuring connectors, consoles, and other clients.

  Micro Focus recommends using the fully-qualified domain name.
- If you do not want the host name on your DNS server, add a static host entry to the `/etc/hosts` file to resolve the host name locally.

To install software ESM in compact mode:

1. Ensure that the license file is accessible and type **yes**.
2. Select the language for interface displays.
3. Specify **0** to install ESM in compact mode.
4. For **CORR-Engine Password**, complete the following:
   a. Press **Enter** to continue with obfuscated passwords or type **no** to display passwords.
   b. Specify a password for the CORR-Engine and verify the password.

      For information about password restrictions, see the Administrator's Guide.
5. For **CORR-Engine Configuration**, specify the following information:
   a. **System Storage Size** - amount of storage space to set aside for storing resources
   b. **Event Storage Size** - amount of storage space to set aside for storing events
   c. **Online Event Archive Size** - maximum number of gigabytes of disk space for event archives
   d. **Retention Period** - amount of time that you want to retain events before they are purged from the system
6. For **Notification Emails**, specify the following information:
   a. Specify an email account to receive email notifications if the Manager becomes unavailable or encounters some other problem.

      You can use the Manager Configuration Wizard to specify more email addresses. For more information, see the Administrator's Guide.
   b. Specify an email address for the sender of notification emails.

      Notification emails will be sent in the following situations:
      - The subsystem status changes. The email includes information about the the change and who made it.
      - The report is successfully archived.
      - The account password is reset.
      - The archive report generation fails.
      - A destination receives too many notifications.
      - The event archive location reaches the cap space. The notification requests that you free up space by moving the event archives to another location.
      - The user elects to email the ArcSight Console settings.
      - The user sends a partition archival command.

- An archive fails because there is not enough space.
- The connection to the database fails.

7. Provide the path and file name of the license file that you downloaded.
8. Select whether to install in default mode or FIPS mode.

Note: FIPS 140-2 mode is the default selection.

Regardless of the mode you select, ensure that ESM and connectors use the same mode.

Caution:

- If you choose to install in FIPS mode, you must also install the ArcSight Console in FIPS mode. For more information, see Installing the ArcSight Console in FIPS Mode.
- After you configure ESM in FIPS mode, you cannot convert it to default mode without reinstalling it.
- Converting from default mode installation to FIPS-140-2 mode is supported. For more information, see the Administrator's Guide.
- By default, ESM uses a self-signed certificate. To use a CA-signed certificate, you must import the CA-signed certificate manually **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.

9. If you selected to install in FIPS mode, select the cipher suite.

   Suite B defines two security levels of 128 and 192 bits. The security levels are based on the Advanced Encryption Standard (AES) key size that is used instead of the overall security provided by Suite B. At the 128-bit security level, the 128 bit AES key size is used. However, at the 192-bit security level, a 256 bit AES key size is used. Although a larger key size means more security, it also means computational cost in time and resource (CPU) consumption. In most scenarios, the 128-bit key size is sufficient.
10. Specify the following information for the ArcSight Manager:
    a. Host name
    b. Credentials for the admin user

    For considerations that apply to the Manager host name, see Installing Software ESM in Compact Mode Using the Configuration Wizard.

    By default, the Manager uses a self-signed certificate. To use a CA-signed certificate, you must import the CA-signed certificate manually **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.
11. Specify the global event ID generator ID that will be used to generate global event IDs.

You must specify an integer between 0 and 16384 (0 and 16384 are not valid). For more information, see Specifying a Global Event ID Generator ID.

12. If Transformation Hub is part of your ESM implementation, select whether to set up a connection to it.

    For more information, see the applicable topic:

    - Configuring Transformation Hub Access - Non-FIPS Mode
    - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode
    - Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)
    - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

    Note: If ESM will connect to Kafka using SASL/PLAIN authentication, skip this step and use `managersetup` to configure the connection after you complete the initial configuration. For more information, see Completing Post-Installation Tasks.

    If you select to set up a connection, provide the following information:

    a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

       Note: You must specify the host name and *not* the IP address.

       Transformation Hub can only accept IPv4 connections from ESM.

    b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

       Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2).

       For more information, see the Administrator's Guide for the ArcSight Platform.

    c. Import the Transformation Hub root certificate to ESM's client truststore.

       Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Copy the Transformation Hub root certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` on the Transformation Hub server to a local folder on the ESM server. After you provide the path to the certificate, the wizard imports the Transformation Hub root certificate into ESM's client truststore and validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

13. Select whether to integrate Recon.

    If you select to integrate, specify the **Search URL** for the Recon deployment.

    Note: ArcSight ESM version 7.5 requires Recon 1.1.0.

14. (Conditional) If you want to integrate with the ServiceNow® IT Service Management (ITSM) application, click **Yes**, and then complete the following:

    a. Specify the mandatory **ServiceNow URL** and the optional **ServiceNow Proxy URL**.

    For information about completing the configuration, see Configuring Integration with ServiceNow®.

    b. (Conditional) If you want to use a global ID to authenticate connections to ServiceNow, click **Yes**, and then specify the user name and password.

15. If you are not licensed to use optional packages, press **Enter** to advance to the next screen. Otherwise, select the optional packages that you are licensed to use. In addition to these optional packages, default standard content packages are installed automatically on the ArcSight Manager. These default packages provide essential system health and status operations, and you can use them immediately to monitor and protect your network.

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

16. Select to continue with the installation. You will receive a message when the installation is complete.

17. Log in as user `root` and run the following script to set up and start the required services:

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

18. Check the location and size of your storage volumes and use ArcSight Command Center to make any necessary changes. For more information, see the Command Center User's Guide.

Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard

This section describes installing ESM in distributed correlation mode. Before you install ESM in distributed correlation mode, review the information in Planning for a Distributed Correlation Cluster. You must also prepare the system to run the information repository on a partition that does not contain `/opt/arcsight`. For more information, see Placing Information Repository Instances on a Separate Partition.

For information about configuring and managing the cluster after you install ESM, see the Administrator's Guide.

When you install ESM in distributed correlation mode, you must first install ESM on the persistor node (by default, the node on which you install ESM first). For more information, see Installing ESM on the Persistor Node. After you install ESM on the persistor node, install it on the other cluster nodes as needed and then perform post-installation configuration tasks. For more information, see Adding Nodes to a Cluster and Configuring the Cluster .

Do not attempt to install ESM on multiple nodes at the same time. You must install ESM on the persistor node and then add additional nodes one at a time.

If necessary, you can manually run the configuration wizard again if you exit the wizard before you reach the About to Configure screen. For more information, see Re-running the ESM Configuration Wizard.

Installing ESM on the Persistor Node

Note: If you have a High Availability (HA) implementation, HA is supported only on the persistor node in the distributed correlation cluster. HA is not supported on any non-persistor node in a distributed correlation cluster.

During the installation, the wizard prompts you to specify the ArcSight Manager host name. Keep the following points in mind when specifying the host name:

- The Manager host name is used to generate a self-signed certificate. The Common Name (CN) in the certificate is the host name that you specify when prompted.
- The Manager host name is the IP address (for IPv4 only) or the fully-qualified domain name of the server where the Manager is installed. All clients (for example, the ArcSight Console) use this name to connect to the Manager. For flexibility, Micro Focus recommends using a fully-qualified domain name instead of an IP address.

- If you are installing on a dual-stack system, the wizard prompts you to select the preferred IP protocol. Your selection controls the following:
  - The IP address that third-party software uses if a host name is given. For example, the email server in Manager Setup.
  - The IP address that is used on the peering page if a host name is given.
  - Whether an IPv4 or an IPv6 address is used for the manager asset.
- The Manager might have more than one host name, and the default name might not be the same as the name that the `hostname` command returns. If you are using the High Availability module, use the service host name that is common to both systems (primary and secondary) as the Manager host name. Otherwise, choose the name that you expect to work and that is convenient for configuring connectors, consoles, and other clients.

  Micro Focus recommends using the fully-qualified domain name.
- If you do not want the host name on your DNS server, add a static host entry to the `/etc/hosts` file to resolve the host name locally.

To install ESM on the persistor node:

1. If you are installing in console mode, start the configuration wizard:

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

2. Ensure that the license file is accessible and accept the license agreement.
3. Select the language for interface displays.
4. Specify **1** to install ESM in distributed mode.
5. Specify **0** to start a new cluster.

   Starting a new cluster creates the first node in the cluster. This node is the persistor node and contains a built-in distributed cache and the information repository.
6. Specify the lowest and highest port numbers for the cluster. The default values are as follows:
   - Lowest ESM server port: 10000
   - Highest ESM server port: 10100

   You must specify a range of available ports for your cluster. This range of ports is made available for dynamic assignment to services (aggregator and correlator, message bus data and message bus control, and distributed cache) as they are added to a cluster. The lowest valid value is 1024 and the highest valid value is 32767. The difference between the lowest value and the highest value must be at least 100.
7. For **Certificate Administrator Master Password**, complete the following:

a. Press **Enter** to continue with obfuscated passwords or type **no** to display passwords.

b. Specify a password for the certificate administrator and verify the password.

   For information about password restrictions, see the Administrator's Guide.

8. For **CORR-Engine Password**, specify a password for the CORR-Engine and verify the password.

   For information about password restrictions, see the Administrator's Guide.

9. For **CORR-Engine Configuration**, specify the following information:

   a. **System Storage Size** - amount of storage space to set aside for storing resources

   b. **Event Storage Size** - amount of storage space to set aside for storing events

   c. **Online Event Archive Size** - maximum number of gigabytes of disk space for event archives

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

10. For **Notification Emails**, specify the following information:

    a. Specify an email account to receive email notifications if the ArcSight Manager becomes unavailable or encounters some other problem.

       You can use the Manager Configuration Wizard to specify more email addresses. For more information, see the Administrator's Guide.

    b. Specify an email address for the sender of notification emails.

       Notification emails will be sent in the following situations:

       - The subsystem status changes. The email includes information about the change and who made it.
       - The report is successfully archived.
       - The account password is reset.
       - The archive report generation fails.
       - A destination receives too many notifications.
       - The event archive location reaches the cap space. The notification requests that you free up space by moving the event archives to another location.
       - The user elects to email the ArcSight Console settings.
       - The user sends a partition archival command.
       - An archive fails because there is not enough space.
       - The connection to the database fails.

11. Provide the path and file name of the license file that you downloaded.

12. Select whether to install in default mode or FIPS mode.

Note: FIPS 140-2 mode is the default selection.

Regardless of the mode you select, ensure that ESM and connectors use the same mode.

Caution:

- If you choose to install in FIPS mode, you must also install the ArcSight Console in FIPS mode. For more information, see Installing the ArcSight Console in FIPS Mode.
- After you configure ESM in FIPS mode, you cannot convert it to default mode without reinstalling it.
- Converting from default mode installation to FIPS 140-2 mode is supported. For more information, see the Administrator's Guide.
- By default, ESM uses a self-signed certificate. To use a CA-signed certificate, you must manually import the CA-signed certificate **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.

13. If you selected to install in FIPS mode, select the cipher suite.

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

14. Specify the following information for the ArcSight Manager:

    a. Host name

    b. Credentials for the admin user

    For considerations that apply to the Manager host name, see Installing ESM on the Persistor Node.

    By default, the Manager uses a self-signed certificate. To use a CA-signed certificate, you must manually import the CA-signed certificate **after** the configuration wizard completes successfully. For information about using a CA-signed certificate, see the Administrator's Guide.

15. Specify the global event ID generator ID that will be used to generate global event IDs.

    You must specify an integer between 0 and 16384 (0 and 16384 are not valid). For more information, see Specifying a Global Event ID Generator ID.

16. If Transformation Hub is part of your ESM implementation, select whether to set up a connection to it.

    For more information, see the applicable section:

- Configuring Transformation Hub Access - Non-FIPS Mode
- Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode
- Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)
- Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

Note: If ESM will connect to Kafka using SASL/PLAIN authentication, skip this step and use `managersetup` to configure the connection after you complete the initial configuration. For more information, see Completing Post-Installation Tasks.

If you select to set up a connection, provide the following information:

a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

Note: You must specify the host name and *not* the IP address.

Transformation Hub can only accept IPv4 connections from ESM.

b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

For more information, see the Administrator's Guide for the ArcSight Platform.

Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2).

c. Import the Transformation Hub root certificate to ESM's client truststore.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Copy the Transformation Hub root certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` on the Transformation Hub server to a local folder on the ESM server. After you provide the path to the certificate, the wizard imports the Transformation Hub root certificate into ESM's client truststore and validates the connection to Transformation Hub. If there

are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

17. Select whether to integrate Recon.

    If you select to integrate, specify the **Search URL** for the Recon deployment.

    Note: ArcSight ESM version 7.5 requires Recon 1.1.0.

18. (Conditional) If you want to integrate with the ServiceNow® application, click **Yes**, and then complete the following:

    a. Specify the mandatory **ServiceNow URL** and the optional **ServiceNow Proxy URL**.

       For information about completing the configuration, see Configuring Integration with ServiceNow®.

    b. (Conditional) If you want to use a global ID to authenticate connections to ServiceNow, click **Yes**, and then specify the user name and password.

19. If you are not licensed to use optional packages, press **Enter** to advance to the next screen. Otherwise, select the optional packages that you are licensed to use. In addition to these optional packages, default standard content packages are installed automatically on the ArcSight Manager. These default packages provide essential system health and status operations, and you can use them immediately to monitor and protect your network.

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

20. Select the distributed correlation services to implement:

    - **0: Distributed Cache** - configures silently
    - **1: Correlation** - allows you to add aggregators and correlators to the cluster on the node you are installing. The wizard runs later in the installation.

21. Select to continue with the installation. You will receive a message when the installation is complete.

    If you chose to add aggregators and correlators to the cluster, the ArcSight Correlation Configuration Wizard runs. For information about completing the wizard, see the Administrator's Guide.

22. To set up the services, log in as user `root` and run the following script:

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

    Note: In the context of distributed correlation setup, `setup_services` does not start services. Do not start services until all cluster configuration is complete.

To add cluster nodes, see Adding Nodes to a Cluster.

After adding cluster nodes, see Configuring the Cluster for information about additional tasks.

Adding Nodes to a Cluster

After you install the persistor node, you can add nodes to the cluster. Micro Focus recommends starting with a four-node or five-node cluster, as these cluster sizes have been tested, but you are not limited to five nodes and can initially install more than five.

To add nodes to the cluster:

1. For each node that you want to add, complete the steps in Running the Installation File.
2. If you are installing in console mode, start the configuration wizard:

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

3. Select the language for interface displays.
4. Specify **1** to install ESM in distributed mode.
5. Specify **1** to add to a cluster.
6. Provide the host name or IP address of the system on which you installed an information repository node, normally the persistor node.

   Note: If the cluster is in pure IPv6 mode, where only IPv6 addresses are available in the interface, you must enter the host name of an information repository node. Using the IP address with an IPv6 system is not supported for cluster configuration.

7. Select the distributed correlation services to implement:
   - **0: Distributed Cache** - configures silently
   - **1: Correlation** - allows you to add aggregators and correlators to the cluster on the node you are installing. The wizard runs later in the installation.
8. Select to continue with the installation. You will receive a message when the installation is complete.

   If you chose to add aggregators and correlators to the cluster, the ArcSight Correlation Configuration Wizard runs. For information about completing the wizard, see the Administrator's Guide.
9. To set up the services, log in as user `root` and run the following script:

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

   Note: In the context of distributed correlation setup, `setup_services` does not start services. Do not start services until all cluster configuration is complete.

After you add nodes to the cluster, see Configuring the Cluster for information about additional tasks.

Configuring the Cluster

Perform this task on the persistor node.

To configure the cluster:

1. Configure passwordless SSH.

   This is required for the operation of message bus data and message bus control instances in the distributed correlation cluster. For more information, see Setting Up Key-Based Passwordless SSH - Distributed Correlation Mode Only.

2. Approve certificates.

   The cluster nodes use certificates to enable communication between the nodes. Each time you add a node to a cluster, ESM creates an entry for that node in the information repository. To approve certificates:

   a. As user `arcsight`, run the following command:

   ```
   /opt/arcsight/manager/bin/arcsight certadmin -list submitted
   ```

   Review the output to verify that the certificates represent the cluster nodes. To view the certificate details, use the `-v` option.

   b. After you confirm that the certificate list is correct, run the following command:

   ```
   /opt/arcsight/manager/bin/arcsight certadmin -approveall
   ```

   Specify the cluster administration password that was provided when you installed ESM on the persistor node.

3. Stop all services:

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

4. Start the information repository:

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

5. Configure message bus data and message bus control instances:

   a. Run `<ARCSIGHT_HOME>/bin/arcsight mbussetup`. The command starts the configuration wizard on the persistor node, but does not add a message bus instance on the persistor node. Add message bus data and message bus control instances to non-persistor nodes.

   b. Select **I want to add, delete, or change an instance**.

c. Enter the number of `mbus_data` instances you want on each node.

   You need a minimum of three message bus data instances per cluster.

d. Enter the number of `mbus_control` instances you want on each node.

   Add one or three instances of the message bus control service per cluster.

6. Configure additional information repository instances:

   Note: Most configurations benefit from three information repository instances. A cluster can have either one repository instance or three instances, with one repository instance per node. Other numbers of repository instances are not supported.

   If you are running the APHA module, it is not necessary to add `repo` instances. After you start the services, ESM automatically converts the cluster to have three `repo` instances, all on non-persistor nodes.

   a. Run `<ARCSIGHT_HOME>/bin/arcsight reposetup`.

   b. Select **Change the list of Information Repository Instances**.

   c. From the list of existing nodes, select two nodes to add a total of three repositories.

7. As user `arcsight`, start the services:

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

8. Verify that all services are running:

```
/etc/init.d/arcsight_services statusByNode
```

Setting Up Key-Based Passwordless SSH - Distributed Correlation Mode Only

The distributed correlation services cluster depends on key-based passwordless SSH to enable communication among the cluster services. In the distributed correlation environment, passwordless SSH must be implemented on the node in the cluster that contains the persistor.

The command `arcsight_services` uses passwordless SSH to allow starting and stopping of services on remote nodes through commands originating on the persistor node. In this instance, passwordless SSH works by generating a keypair on the persistor, and configuring the remote node to accept the login based on a public key for the Persistor node. In the distributed correlation environment, ESM is configured to allow the user `arcsight` on the persistor node to connect to a remote node as the user `arcsight` . Only `arcsight` user to `arcsight` user passwordless SSH is supported, and only from the persistor node to other cluster nodes.

Set Up Key-Based Passwordless SSH

After installing ESM on all nodes, use this command on the persistor node to setup passwordless SSH with cluster nodes:

```
/etc/init.d/arcsight_services sshSetup
```

If a node needs configuration, the command prompts you for the user `arcsight` password on the node, so it can log in and complete the setup.

Verify Key-Based Passwordless SSH

On the persistor node, run the command `/etc/init.d/arcsight_services checkSshSetup`. This command verifies whether the nodes in the cluster are configured with passwordless SSH.

Handling a Time Zone Update Error

There are two possible errors that can occur when the installation program tries to update time zone information for the ESM components:

- A time zone version 2019b or later rpm for your operating system is not installed.
- The `/etc/localtime` link is pointing to an invalid or non-existent time zone.

You can choose to continue with the installation even if there are errors with the time zone package. If so, you can install the correct time zone package after the ESM installation completes. For more information, see Installing the Time Zone Update Package

Chapter 4: Completing Post-Installation Tasks

After you confirm that the installation was successful, complete the applicable tasks in this chapter. Depending on your configuration, some tasks might not apply.

After you complete the applicable post-installation tasks, install the ArcSight Console. For more information, see Installing ArcSight Console.

To complete post-installation tasks:

1. Configure reports to display in a non-English environment.

   To enable queries to retrieve international characters in string-based event fields, you must ensure that you store the characters correctly. For more information, see Configuring Reports to Display in a Non-English Environment.
2. If you are running software ESM, tune the BIOS to improve performance.

   For more information, see Tuning the BIOS.
3. If you want to connect a browser to a FIPS web server, configure the browser to support TLS by turning off SSL protocols and turning on TLS protocols.

   For example, in Internet Explorer:

   a. Select **Tools** > **Internet Options**.

   b. Select the **Advanced** tab.

   c. In the Security section, uncheck **Use SSL 2.0** and **Use SSL 3.0**.

   d. Select the appropriate TLS options. For more information, see TLS Support.
4. If you are running ESM in distributed correlation mode, add or remove cluster services as desired.

   ESM supports dynamic addition and removal of the following cluster services:

   - Aggregator
   - Correlator
   - Distributed cache (`dcache`)
   - Information repository (`repo`)

   After you add a service, as user `arcsight`, run the following command to start the service:

   ```
   /etc/init.d/arcsight_services start <service ID>
   ```

   If you want to configure a new node and add services, as user `arcsight`, you must stop and start all of the ESM services:

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

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

Before you remove a service, you must stop the service.

For more information about adding cluster services, see the Administrator's Guide.

5. Install the ArcSight Platform.

   The ArcSight Platform enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment:

   - Real-time event monitoring and correlation with data from ESM
   - Analyzing end-user behavior with Interset

   To help you get started, the ArcSight Platform provides a Dashboard with a set of out-of-the-box widgets and dashboards. Users can organize the widgets into personalized dashboards.

   For information about deploying, configuring, and maintaining this product, see the ESM Release Notes and the Administrator's Guide for the ArcSight Platform.

   Note: This release allows you to connect to a single ESM instance.

6. If you want the ability to view Command Center from the ArcSight Platform, install ESM in the ArcSight Platform and then configure the ESM host in the ArcSight Platform. For more information, see the Administrator's Guide for the ArcSight Platform.

   This feature allows you to view Command Center from the ArcSight Platform without having to switch to the ESM host for Command Center. After you install ESM and configure the host in the ArcSight Platform, refresh the dashboard to display the Command Center menu in the ArcSight Platform. Click the menu to start Command Center. To go back to the ArcSight Platform dashboard from Command Center, use the ArcSight Platform menu from the Dashboard menu in Command Center.

7. Configure Transformation Hub access.

   For more information, see the applicable topic:

   - Configuring Transformation Hub Access - Non-FIPS Mode
   - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode
   - Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)
   - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

8. Configure integration with ServiceNow® IT Service Management (ITSM).

For more information, see Configuring Integration with ServiceNow®.

9. To change the method for authenticating users with the ArcSight Manager:
   a. As user `arcsight`, stop the ArcSight Manager:

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

   b. As user `arcsight`, from the `/opt/arcsight/manager/bin` directory, run the following command to start the `managersetup` wizard:

      ```
      ./arcsight managersetup -i console
      ```

   c. Advance through the wizard until you reach the authentication options screen.
   d. Select one of the following methods for authenticating users with the ArcSight Manager:
      - **Password Based Authentication**

        Log in with a user name and password.
      - **Password Based and SSL Client Based Authentication**

        Base authentication on the user name and password combination *or* the authentication of the client certificate by the Manager.
      - **SSL Client Only Authentication**

        Manually set up the authentication of the client certificate by the Manager.
      - **OSP Client Only Authentication**

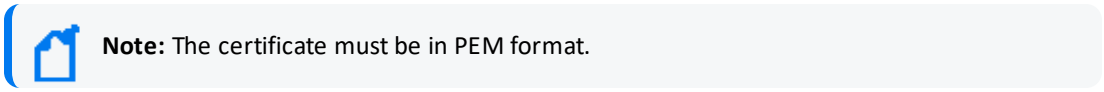
        Allow ESM to use an existing One SSO Provider (OSP) (for example, from the ArcSight Platform) for authentication.

        Note: If you select this method, when you register a connector with ESM, specify the ESM user credentials and not the OSP credentials.
      - **External SAML2 Client Only Authentication**

        Configures the SAML2 client that is embedded in ESM to establish a trust relationship with your own external identity provider.

        Note: If you select this method, when you register a connector with ESM, specify the ESM user credentials and not the OSP credentials.
   e. If you selected **OSP Client Only Authentication**, provide the following information:
      - Host name and port of the OSP server
      - Tenant name that you specified for the OSP
   f. If you selected **External SAML2 Client Only Authentication**, provide the following information:

- Either the SAML2 metadata URL or the location of the SAML2 metadata file to be uploaded
- Location of the certificate that the external identity provider uses for signing SAML2 requests



After configuration of the External SAML2 Client Only Authentication method is complete and you restart the manager, you can find the manager's metadata at `https://<manager-host-name:manager-port>/osp/a/esm/auth/saml2/spmetadata`.

g. Advance through the wizard and complete the configuration.

For more information about `managersetup`, see the Administrator's Guide.

h. If you are running in FIPS mode and using External SAML2 Client Only Authentication, run the `migrate_fips_osp_keystore` script to update the keystore that the OSP uses:

```
/opt/arcsight/manager/bin/arcsight migrate_fips_osp_keystore
```

i. As user `arcsight`, restart the ArcSight Manager:

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

Configuring Reports to Display in a Non-English Environment

The tasks in this section apply only if you plan to generate PDF reports that use international characters. The `ARIALUNI.TTF` font is required to configure the reports.

To configure reports to display international characters:

1. On the ArcSight Manager host, place the `ARIALUNI.TTF` file in the appropriate folder. For example, `/usr/share/fonts/<your folder>`.
2. Add the following line to the `sree.properties` file, located in the `/opt/arcsight/manager/reports/` directory by default:

```
font.truetype.path=/usr/share/fonts/<your folder>
```

3. Stop and start the ArcSight Manager:

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

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

4. On the ArcSight Console host operating system, install the Arial Unicode MS font if it is not already present.
5. From `<ARCSIGHT_HOME>/current/bin/scripts`, modify `console.bat` (on Windows) or `console.sh` (on Macintosh) to append the JVM option `" -Dfile.encoding=UTF8"` to the `ARCSIGHT_JVM_OPTIONS` section.

   Note: The coding is set correctly on Linux. Modifications are not required.
6. From the console **Preferences** menu (**Edit** > **Preferences** > **Global Options** > **Font**), set Arial Unicode MS as the default font.
7. Set font preferences for your reports.

   For more information, see the ArcSight Console User's Guide.

Tuning the BIOS

If you are running software ESM, you can tune the BIOS to improve server performance.

To tune the BIOS:

1. Disable **HyperThreading**.

   This setting exists on most server class processors (for example, Intel processors) that support hyper threading. AMD processors do not have an equivalent setting.
2. Disable **Intel VT-d**.

   This setting is specific to Intel processors and is likely to be present on most recent server class processors. AMD processors have an equivalent setting called AMD-Vi.
3. Set **Power Regulator** 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 recent CPUs have an equivalent setting.
4. Set **Thermal Configuration** to **Increased Cooling**.

   This setting increases the server fan speed to avoid issues with the increased heat that results from constantly running the CPU(s) at high speed.
5. Enable the **Minimum Processor Idle Power Package State** setting.

   This setting tells the CPU not to use any of its C-states (various states of power saving in the CPU).
6. Set **Power Profile** to **Maximum Performance**.

   This setting results in the following changes:

- QPI power management (the link between physical CPU sockets) is disabled.
- PCIe support is forced to Gen 2.
- C-states are disabled.
- Lower speed settings on the CPUs are disabled so that the CPUs constantly run at high speed.

Configuring Transformation Hub Access - Non-FIPS Mode

This section describes how to configure ESM to access Transformation Hub when FIPS mode is *not* enabled.

To configure ESM access to Transformation Hub in non-FIPS mode:

1. As user `arcsight`, stop the ArcSight Manager:

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

2. As user `arcsight`, from the `/opt/arcsight/manager/bin` directory, run the following command to start the `managersetup` wizard:

   ```
   ./arcsight managersetup -i console
   ```

   Advance through the wizard until you reach the Transformation Hub screen.

3. Provide the following information:

   a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all worker nodes. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

   > **Note:** You must specify the host name and *not* the IP address.
   >
   > Transformation Hub can only accept IPv4 connections from ESM.
   >
   > If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

   b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

   For more information, see the Administrator's Guide for the ArcSight Platform.

> **Note:** You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

c. Import the Transformation Hub root certificate to ESM's client truststore.

   Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

   On the Transformation Hub master node, run the following command to generate the `ca.crt` root certificate file in the `/tmp` folder:

   ```
   /opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt
   ```

   Copy `/tmp/ca.crt` to a local folder on the ESM server. After you provide the path to the certificate, the wizard imports the Transformation Hub root certificate into ESM's client truststore

d. If the Kafka cluster is not configured to use SASL/PLAIN authentication, leave the authentication type as None. If the Kafka cluster is configured to use SASL/PLAIN authentication, select SASL/PLAIN as the authentication type.

e. If you selected SASL/PLAIN as the client authentication type, specify the user name and password for authenticating to Kafka.

f. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <host name:port>.

   Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

   The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topic that you specified, and verify that the topic contains Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topic that you specified and compare it to the `Event 1.0.0` schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

g. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use

filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them.
- Filter out ESM's correlation events that were forwarded (CEF events that the Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own events.

If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For information about configuring filters or local and global event enrichment in Transformation Hub, see the Administrator's Guide for the ArcSight Platform.

The wizard validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

4. Advance through the wizard and complete the configuration.

   For more information about `managersetup`, see the Administrator's Guide.

5. As user `arcsight`, restart the ArcSight Manager:

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

6. To verify that the connection to Transformation Hub is working, look for the following line in `server.log`:

   ```
   Transformation Hub service is initialized
   ```

Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode

Before setting up client-side authentication with Transformation Hub, you must import the Transformation Hub root certificate into the ESM truststore.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Note: You must specify the Transformation Hub host name and *not* the IP address when configuring Transformation Hub access.

To import the Transformation Hub root certificate into an ESM truststore:

Note: Before completing the steps below, verify whether the Transformation Hub root certificate has previously been imported into ESM. If it has, you do not need to re-import it.

1. From the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
2. Use the `keytool` command to import the root CA certificate into the ESM truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file /tmp/ca.crt -alias alias1
   ```

To enable client-side authentication between Transformation Hub and ESM:

1. Obtain your company's root CA certificate, an intermediate certificate, and key pair and place them in `/tmp` with the following names:
   - `/tmp/intermediate.cert.pem`
   - `/tmp/intermediate.key.pem`
   - `/tmp/ca.cert.pem`
2. Verify that Transformation Hub is functional and that client authentication is configured.
3. As user `arcsight`, stop the ArcSight Manager:

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

4. If `/opt/arcsight/manager/config/client.properties` does not exist, create it using an editor of your choice.
5. Change the store password for the keystore, `keystore.client`, which has an empty password by default. This empty password interferes with the certificate import:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -storepasswd
   -storepass ""
   ```

6. Run the following command to update the empty password of the generated key

`services-cn` in the keystore to be the same password as that of the keystore itself. When prompted, enter the same password that you entered for the store password:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -keypasswd -
keypass "" -alias services-cn
```

7. Run the following command to update the password in `config/client.properties`:

```
/opt/arcsight/manager/bin/arcsight changepassword -f
config/client.properties -p ssl.keystore.password
```

8. Generate the keypair and certificate signing request (`.csr`) file. When generating the keypair, enter the fully qualified domain name of the ArcSight Manager host as the common name (CN) for the certificate.

   Run the following commands:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair
–dname "cn=<your host's fully qualified domain name>, ou=<your
organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize
2048 –alias ebkey -startdate -1d -validity 366
```

```
/opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
alias ebkey -file ebkey.csr
```

   where `ebkey.csr` is the output file where the `.csr` is stored.

9. Sign the `.csr` with the Transformation Hub root certifcate. On the Transformation Hub server, the root certificate is located at `/opt/arcsight/kubernetes/ssl/intermediate.cert.pem` and the key is called `ca.key`.

   Run the following command on either the Transformation Hub server or a different server with a functional `openssl` (as long as you have the `intermediate.cert.pem` and `intermediate.key.pem` available):

```
openssl x509 -req -CA ${INTERMEDIATE_CA_CRT} -CAkey ${INTERMEDIATE_CA_
KEY} -in <full path to the esm csr> -out <full path and file name for
storing the generated cert> -days 3650 -CAcreateserial -sha256
```

   For example:

```
openssl x509 -req -CA /tmp/intermediate.cert.pem -CAkey
/tmp/intermediate.key.pem -in /tmp/ebkey.csr -out
/tmp/signedIntermediateEBkey.crt -days 3650 -CAcreateserial -sha256
```

   You must specify all file locations with the full path.

10. Import the intermediate certificate and CA certificate from Transformation Hub into the ESM client truststore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
<alias for the certificate> -importcert -file <absolute path to
certificate file>
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
thintcert -importcert -file /tmp/intermediate.cert.pem
```

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
thcert -importcert -file /tmp/ca.cert.pem
```

11. On the ESM server, run the following command to import the signed certificate (the `-out` parameter in the above `openssl` command):

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
-importcert -file <path to signed cert> -trustcacerts
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
-importcert -file /tmp/signedIntermediateEBkey.crt -trustcacerts
```

12. To verify that the configuration is complete and that the connection to Transformation Hub is valid, run `managersetup` and ensure that there are no errors.
13. Start the ArcSight Manager:

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

Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)

This section describes how to configure ESM to access Transformation Hub when FIPS mode is enabled. FIPS 140-2 is the only supported FIPS mode.

To configure ESM access to Transformation Hub in FIPS Mode:

1. As user `arcsight`, stop the ArcSight Manager:

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

2. From the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
3. Use the `keytool` command to import the root CA certificate into the ESM client truststore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
-file <absolute path to certificate file> -alias <alias for the
certificate>
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
-file /tmp/ca.crt -alias alias1
```

4. As user `arcsight`, run the following command from the `/opt/arcsight/manager/bin` directory to start the `managersetup` wizard:

```
./arcsight managersetup -i console
```

For more information about `managersetup`, see the Administrator's Guide.

5. Provide the following information:

Note: You do not need to provide the path to the Transformation Hub root certificate, as it has already been imported.

a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

Note: You must specify the host name and *not* the IP address.

Transformation Hub can only accept IPv4 connections from ESM.

If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

For more information, see the Administrator's Guide for the ArcSight Platform.

Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

c. If the Kafka cluster is *not* configured to use SASL/PLAIN authentication, leave the authentication type as None. If the Kafka cluster is configured to use SASL/PLAIN authentication, select SASL/PLAIN as the authentication type.

d. If you selected SASL/PLAIN as the client authentication type, specify the user name and password for authenticating to Kafka.

e. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <host name:port>.

Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topics that you specified, and verify that the topics contain Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topics that you specified and compare them to the schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

f. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them
- Filter out ESM's correlation events that were forwarded (CEF events that the Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own events.

If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For information about configuring filters or local and global event enrichment in Transformation Hub, see the Administrator's Guide for the ArcSight Platform.

The wizard validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

6. Advance through the wizard and complete the configuration.
7. As user `arcsight`, restart the ArcSight Manager:

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

8. To verify that the connection to Transformation Hub is working, look for the following line in `server.log`:

```
Transformation Hub service is initialized
```

Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - FIPS Mode

Before setting up client-side authentication with Transformation Hub, you must import the Transformation Hub root certificate into the ESM truststore and the Transformation Hub intermediate certificate into the ESM keystore. Before you begin this task, verify whether the certificates have previously been imported into ESM. If they have, you do not need to re-import them.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Note: You must specify the Transformation Hub host name and *not* the IP address when configuring Transformation Hub access.

To enable client-side authentication between Transformation Hub and ESM:

1. Copy `ca.cert.pem` and `intermediate.cert.pem` from Transformation Hub to a location on the ESM server.
2. From the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
3. Use the `keytool` command to import the root CA certificate into the ESM truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file /tmp/ca.crt -alias alias1
   ```

4. Use the `keytool` command to import the intermediate certificate into the ESM keystore:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -importcert
-file <absolute path to certificate file> -alias <alias for the
certificate>
```

For example:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -importcert
-file /tmp/intermediate.cert.pem -alias alias2
```

5. As user `arcsight`, stop the ArcSight Manager:

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

6. Generate a keypair:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair
-dname "cn=<fully-qualified domain name of the host>, ou=<organizational
unit>, o=<organization name>, c=<country code>" -keyalg rsa -keysize 2048
-alias <alias name> -startdate -1d -validity 366
```

7. Generate a certificate signing request file:

```
/opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
alias <alias name> -file <filename>.csr
```

8. Copy the `.csr` file to the Transformation Hub master node.
9. On the Transformation Hub master node, generate the signed certificate:

```
openssl x509 -req -CA /opt/intermediate_cert_files/intermediate.cert.pem
-CAkey /opt/intermediate_cert_files/intermediate.key.pem -in /opt/<file
name>.csr -out /opt/<file name>.crt -days 3650 -CAcreateserial -sha256
```

10. Copy the signed certificate to the ESM server.
11. On the ESM server, import the signed certificate:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias
<alias name> -importcert -file <absolute path to the certificate file> -
trustcacerts
```

12. As user `arcsight`, run the following command from the `/opt/arcsight/manager/bin` directory to start the `managersetup` wizard:

```
./arcsight managersetup -i console
```

For more information about `managersetup`, see the Administrator's Guide.

13. Provide the following information:

Note: You do not need to provide the path to the Transformation Hub root certificate, as it has already been imported.

a. Specify the host name and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

> **Note:** You must specify the host name and *not* the IP address.
>
> Transformation Hub can only accept IPv4 connections from ESM.
>
> If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

For more information, see the Administrator's Guide for the ArcSight Platform.

> **Note:** You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2). ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`.

c. If the Kafka cluster is *not* configured to use SASL/PLAIN authentication, leave the authentication type as None. If the Kafka cluster is configured to use SASL/PLAIN authentication, select SASL/PLAIN as the authentication type.

d. If you selected SASL/PLAIN as the client authentication type, specify the user name and password for authenticating to Kafka.

e. If you specified an Avro topic, specify the host name and port for connecting to the Schema Registry in the format <host name:port>.

Transformation Hub runs a Confluent Schema Registry that producers and consumers use to manage compatibility of Avro-format events.

The wizard uses this information to connect to the Schema Registry, read the Avro schemas for the Avro topics that you specified, and verify that the topics contain Avro events that are compatible with ESM. If ESM cannot retrieve the Avro schemas for the Avro topics that you specified and compare them to the schema that is packaged with ESM, or if incompatible schemas are detected, the wizard generates warning messages but allows you to continue. In some cases, you might already know that Transformation Hub will use a compatible schema when the Manager is running.

f. If you choose to configure the Forwarding Connector to forward CEF events to Transformation Hub and then configure Transformation Hub to filter Avro events, use filters to ensure that ESM does not receive duplicate events. You might want to use filters to accomplish the following:

- Filter out desired events from Connectors so that ESM does not process them
- Filter out ESM's correlation events that were forwarded (CEF events that the

Forwarding Connector sent to `th-cef`) so that ESM does not re-process its own events.

If you do *not* configure filtering, ESM must consume from the `th-arcsight-avro` topic. If you configure filtering, ESM must consume from the `mf-event-avro-esmfiltered` topic. For information about configuring filters or local and global event enrichment in Transformation Hub, see the Administrator's Guide for the ArcSight Platform.

The wizard validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

14. Advance through the wizard and complete the configuration.
15. As user `arcsight`, restart the ArcSight Manager:

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

Configuring Integration with ServiceNow®

This section describes how to integrate with ServiceNow® after completing the installation and how to customize the forms for exporting cases and events from ESM to ServiceNow®. ESM can integrate with the ServiceNow® IT Service Management (ITSM) and ServiceNow® Incident Management schemas.

ESM includes configuration files for customizing the export forms in `/opt/arcsight/manager/config/externalCaseManagement` by default. To customize the ITSM export form, use the `SN_ITSM_incident.json` configuration file. To customize the Incident Management export form, use the `SN_SI_incident.json` configuration file. You can customize the export forms as follows:

- Customize field names
- Add or hide fields
- Set required fields
- Map values from ESM cases or events to ServiceNow® ticket fields
- Format fields as drop-down lists
- Configure equality checks between fields

The configuration files include example customizations.

Note: You can export multiple events at the same time. Use the `export.external.ticketsystem.ui.events.max parameter` in the `console.properties` file to specify the maximum number. The default is 10, but you can increase or decrease that setting to meet the needs of your environment. For more information, see the ArcSight Console User's Guide.

To configure ESM to integrate with ServiceNow®:

1. As user `arcsight`, stop the ArcSight Manager services:

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

2. As user `arcsight`, from the `/opt/arcsight/manager/bin` directory, start the `managersetup` wizard:

   ```
   ./arcsight managersetup -i console
   ```

   Advance through the wizard until you reach the ServiceNow® screen.

3. Specify the ServiceNow® URL and, if necessary, the proxy URL that is used to connect to the internet.
4. (Conditional) If you want to use a global ID to authenticate connections to ServiceNow, click **Yes**, and then specify the user name and password.
5. Advance through the wizard and complete the configuration.

   For more information about `managersetup`, see the Administrator's Guide.

6. As user `arcsight`, restart the ArcSight Manager:

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

To customize the export form:

1. Create a back up copy of the `.json` file that you will update (`/opt/arcsight/manager/config/externalCaseManagement/SN_ITSM_incident.json` or `SN_SI_incident.json`).
2. Open `/opt/arcsight/manager/config/externalCaseManagement/SN_ITSM_incident.json` or `SN_SI_incident.json` in a text editor.
3. Ensure that the `main` field is set to `true`.

Note: The `main` field determines the schema to use. Set the field to `true` for only one of the files.

If you change the schema that is in use, modify the `service_name` field in `/opt/arcsight/manager/config/externalCaseManagement/service.json` to reflect the schema that is in use. For example:

- If you are using the ITSM schema, specify `"service_name":"ServiceNow \u00AE ITMS"`.
- If you are using the Incident Management schema, specify `"service_name":"ServiceNow \u00AE SI"`.

4. Modify the appropriate fields.

Use this field...	To modify...
`referenced_table`	the ServiceNow® table that contains the records that you want to reference (for example, sys_user or sys_group) The table must be a valid ServiceNow® table. You must define the table in a separate `.json` file. When you define the table, you must specify at least one field. For an example table definition, see `/opt/arcsight/manager/config/externalCaseManagement/SN_sys_user.json` or `SN_sys_user_group.json`.
`field_type`	the type of data that the field accepts Valid values are `StringField`, `BooleanField`, `DateTimeField`, `IntegerField`, and `NumberField`.
`display_name`	the display name for the field on the export form The name must be less than 20 characters. You can use this field for localization.
`show_in_ui`	the format for the field on the export form Valid values are `FULL_ROW`, `HALF_ROW`, `TEXT_AREA`, and `NONE`. To hide a field, specify `NONE`.
`required`	whether the field is required Valid values are `true` and `false`.

`mappings` for cases	map an ESM case to a ServiceNow® ticket field
	Specify `esm_source` as `case` and `source_field_name` as `<name of ESM case>`. For example:
	`"mappings": [`
	`{`
	`"esm_source": "case",`
	`"source_field_name": "displayId"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "case",`
	`"source_field_name": "name"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "case",`
	`"source_field_name": "description"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "case",`
	`"source_field_name": "summary"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "case",`
	`"source_field_name": "createTime"`
	`}`
	`]`

`mappings` for events	map an event field to a ServiceNow® ticket field
	Specify `esm_source` as `event` and `source_field_name` as `<name of event field>`.
	Some examples of event field mappings:
	`"mappings": [`
	`{`
	`"esm_source": "event",`
	`"source_field_name": "managerReceiptTime"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "event",`
	`"source_field_name": "priority"`
	`}`
	`]`
	`"mappings": [`
	`{`
	`"esm_source": "event",`
	`"source_field_name": "severity"`
	`}`
	`]`

`options`	format the field as a drop-down selection list with the specified values
	There are two methods for formatting a field as a drop-down list. If the display name and the value are the same, use the short form. If the display name and the value are different, use the long form.
	Example 1 (short form):
	`"options": [`
	`"New",`
	`"In progress",`
	`"On hold",`
	`"Resolved",`
	`"Closed",`
	`"Canceled",`
	`]`
	In the short form example above, the label for the first selection in the drop-down list is "New," and the actual value that is assigned is "New."
	Example 2 (long form):
	`"options": [`
	`{`
	`"display": "Low",`
	`"value": 3`
	`},`
	`{`
	`"display": "Medium",`
	`"value": 2`
	`},`
	`{`
	`"display": "High",`
	`"value": 1`
	`}`
	`]`
	In the long form example above, the label for the first selection in the drop-down list is "Low," and the actual value that is assigned is "3."

`checks`	equality checks between fields
	Valid values are `ShouldNotBeEqual` and `ShouldBeEqual`.
	For example:
	`"checks": [`
	`{`
	`"type": "ShouldNotBeEqual",`
	`"columns": [`
	`"<field 1>",`
	`"<field 2>"`
	`},`
	`{`
	`"type": "ShouldBeEqual",`
	`"columns": [`
	`"<field 3>",`
	`"<field 4>"`
	`}`
	`]`

5. Review the modifications and ensure that the format is valid.
6. Save the file, and then stop and start the ArcSight Manager:

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

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

   The customized export forms are available the next time you log in to the ArcSight Console.

Chapter 5: Installing ArcSight Console

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

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

Console Supported Platforms

The hardware requirements for the ArcSight Console are as follows:

	Minimum
Processor	Intel Core i5 2.4 GHz processor
Memory	8 GB RAM (16 preferred)

For the most current information on supported platforms and browsers, see the *Technical Requirements* on the ESM documentation page.

Required Libraries for RHEL and CentOS (64 Bit)

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

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

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

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

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

`libXp-1.0.0-15.1.el6.x86_64.rpm`

`libXp-1.0.0-15.1.el6.i686.rpm`

`libXmu-1.0.5-1.el6.x86_64.rpm`

`libXmu-1.0.5-1.el6.i686.rpm`

`libXft-2.1.13-4.1.el6.x86_64.rpm`

`libXft-2.1.13-4.1.el6.i686.rpm`

```
libXext-1.1-3.el6.x86_64.rpm
libXext-1.1-3.el6.i686.rpm libXrender-0.9.7-2.el6.i686.rpm
gtk2-engines-2.18.4-5.el6.x86_64.rpm
gtk2-2.18.9-6.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.i686.rpm
compat-db-4.6.21-15.el6.x86_64.rpm
compat-db-4.6.21-15.el6.i686.rpm
```

Installing the Console

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

Note: On Linux:

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

Note: On Macintosh:

- Keep in mind that `keytoolgui` does not work on the Mac, so use keytool commands when you need to manage the keystore or certificates. For more information, see the Administrator's Guide.
- Before you start the Console, make sure to set up a default printer to which to print. if you open a channel, select some rows, right-click on them and select **Print Selected Rows** from the resulting menu, the Console will crash if a default printer is not set up.

Make sure that ESM 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. Note that `nnnn` stands for the build number.

Platform	Installation File
Linux	`ArcSight-7.5.0.nnnn.0-Console-Linux.bin`
Windows	`ArcSight-7.5.0.nnnn.0-Console-Win.exe`
Macintosh	`ArcSight-7.5.0.nnnn.0-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" check box is disabled until you scroll to the bottom of the agreement text. After you have read the text, select the "**I accept the terms of the License Agreement**" check box and click **Next**.
5. Read the text in the **Special Notice** panel and click **Next**.
6. On the **Choose ArcSight installation directory** panel, you can accept the default installation directory, click **Choose** to navigate to an existing folder, or type in a path to where you want to install the Console. If you specify a folder that does not exist, the folder is created for you.

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

7. On the **Choose Shortcut Folder** panel, select where you would like to create a shortcut for the Console and uninstall icons and click **Next**.
8. View the summary in the **Pre-Installation Summary** screen and click **Install** if you are satisfied with the paths listed. If you want to make any changes, use the Previous button to do so.

   You can view the installation progress in the progress bar.

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

Configuring the ArcSight Console

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

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

   
   FIPS 140-2 mode is the default selection.

   Select the same mode in which the Manager is installed.

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

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

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

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

   Click **Next**.
3. Enter the Manager host name or IP address of the Manager to which this Console will connect in the **Manager Host Name** field.

   Select the **IP Version** (IPv4 or IPv6) that the Manager is using. If, on a dual stack machine, ESM must be contacted by hostname, and DNS or other naming services have both IPv4 addresses and IPv6 addresses associated with this, the Preferred IP Protocol is used to communicate with ESM.

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

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

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

   Enter the Proxy Host name and click **Next**.
5. The ArcSight Console configuration wizard prompts you to choose the type of client

authentication you want to use. The choices are:

- Password Based Authentication
- Password Based and SSL Client Based Authentication

  Note: This option supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method with this option is not currently supported.

- Password Based or SSL Client Based Authentication

  Caution: In order to use PKCS#11 authentication, you must select this method.

- SSL Client Only Authentication
- OSP Client Only Authentication

  Select this method if ESM will use either OSP Client Only Authentication or External SAML2 Client Only Authentication. For more information about these methods, see the Administrator's Guide.

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 the Administrator's Guide to set up the client certificate.

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

- Client Key Store
- PKCS#11 Token

If you plan to use a PKCS#11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the Console, you can refer to Setting Up to Use a PKCS#11 Provider 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:

Manual setup of the client certificate will be required.
Do you wish to proceed?

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

6. The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Centered Support articles, and other web page content. Specify the location of the executable for the web browser that you want to use to display the Knowledge Centered Support articles and other web pages launched from the ArcSight Console. Browse to and select the **Browser Executable** and click **Next**.
7. Select whether this installation of the Console will be used by a single user or multiple users.

   You can choose from these options:

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

     Select this option when:

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

       OR

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

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

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

   - Multiple users will use this installation

     Select this option when:

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

       AND

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

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

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

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

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

- sendlogs
- console
- exceptions
- portinfo
- websearch

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

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

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

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

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

    where `[language]` is one of the following:
    `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 Console's online help is displayed in a browser. Follow these steps to view the online help if you are using SSL Client Based Authentication mode:

1. Export the keypair from the Console. For more information, see the Administrator's Guide.
2. Import the Console's keypair into the browser.

You have installed the ArcSight Console successfully.

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

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	If you selected Client Keystore as your authentication method, you will see • Login (username and password) • SSL Client Login • Cancel If you selected PKCS#11 Token, you will see • PKCS#11 Login • Login • Cancel
SSL Client Only Authentication	If you selected Client Keystore as your authentication method, you will see • The user ID and Password fields are grayed out (disabled) because login authentication is by client keystore. • Login • Cancel If you selected PKCS#11 Token, you will see • PKCS#11 Login (SSL client authentication) • Cancel

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

Logging into the Console

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

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

Reconnecting to the ArcSight Manager

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

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

Reconfiguring the ArcSight Console

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

On Windows: `arcsight 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 7.5.0.0 Console > Uninstall_ArcSight ESM Console_7.5.0.0** 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 Installation.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 Installation"
```

Alternatively, you can run one of the commands below from `/home/arcsight` (or wherever you installed the shortcut links) directory.

```
./"Uninstall_ArcSight ESM Console_7.5.0.0"
```

or

```
./Uninstall\ Uninstall ArcSight ESM Console Installation
```

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

Chapter 6: Uninstalling ESM and Restarting the Installation Program

This chapter describes how to uninstall ESM (if needed) and run the installation program and configuration wizard again.

Uninstalling ESM

This section describes how to uninstall ESM in compact mode and in distributed correlation mode.

If you are uninstalling ESM in distributed correlation mode, start with the persistor node. After you successfully uninstall the persistor node, uninstall the remaining nodes.

Note: If you are not uninstalling the persistor node, first run the `mbussetup` utility to stop and delete message bus data and message bus control instances from the cluster. Also, run other setup utilities to delete other services from the node. Only run `remove_services.sh` after you run the setup utilities.

To uninstall ESM in compact mode:

1. As user `root`, run the following command:

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

2. As user `arcsight`, shut down any ArcSight processes that are still running:
   a. Check for running ArcSight processes:

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

   b. Shut down any running processes:

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

3. Run the uninstallation program from either the directory where you created the links during installation or, if you did not create links, from the `/opt/arcsight/suite/UninstallerData` directory:

   ```
   ./Uninstall_ArcSight_ESM_Suite_7.5.0.0
   ```

4. Verify that the `/tmp` and `/opt/arcsight` directories do not contain ESM-related files. If the directories do contain ESM-related files, remove them:

a. As user `arcsight`, kill all ArcSight processes.
b. Delete remaining ESM-related directories and files from `/opt/arcsight/` and `/tmp`.
c. Delete any links that were created during installation.

To uninstall ESM in distributed correlation mode:

1. On the persistor node, as user `root`, run the following script to remove services:

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

2. As user `arcsight`, shut down any ArcSight processes that are still running:
   a. Check for running ArcSight processes:

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

   b. Shut down any running processes:

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

3. Run the uninstallation program from either the directory where you created the links during installation or, if you did not create links, from the `/opt/arcsight/suite/UninstallerData` directory:

```
./Uninstall_ArcSight_ESM_Suite_7.5.0.0
```

4. Verify that the `/tmp` and `/opt/arcsight` directories do not contain ESM-related files. If the directories do contain ESM-related files, remove them:
   a. As user `arcsight`, kill all ArcSight processes.
   b. Delete remaining ESM-related directories and files from `/opt/arcsight/` and `/tmp`.
   c. Delete any links that were created during installation.
5. After you uninstall ESM from the persistor node, repeat the process on the remaining nodes. Ensure that you run `remove_services.sh script` on each remaining node.

Re-running the Installation File

For software ESM, if the installation is interrupted, you can re-run the installation file at any time before you reach the File Delivery Complete screen.

To re-run the installation file:

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

3. Run `./ArcSightESMSuite.bin` again.

Re-running the ESM Configuration Wizard

You can re-run the wizard manually only if you exit it **before** the actual configuration begins.

To re-run the configuration wizard:

1. Run the following command:

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

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

   In GUI mode:

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

   In console mode:

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

   If you are running the First Boot Wizard in console mode, ensure that X-Window is **not** running.

   If you encounter a failure during the configuration stage, uninstall and reinstall ESM. On an appliance, restore the appliance to the factory settings and start over. For more information, see Restore Appliance Factory Settings.

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 Customer Support is available if you need it.

If you intend to have 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/var/logs/misc/default/`	Contains detailed troubleshooting information logged during the steps in Installing Software ESM in Compact Mode Using the Configuration Wizard or Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard.
firstbootsetup.log	`/opt/arcsight/var/logs/misc`	Contains brief troubleshooting information about commands that ran during the steps in Installing Software ESM in Compact Mode Using the Configuration Wizard or Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard.
CORR-Engine Log Files		
logger_server.log	`/opt/arcsight/logger/current/arcsight/logger/logs`	Contains troubleshooting information about the CORR-Engine

Log file name	location	Description
logger_ server.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engine stdout log file
arcsight_ logger.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_init_ driver.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_init.sh.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_wizard.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
logger_ wizard.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	Logs for setting up the CORR-Engine
Manager Log Files		
server.log	/opt/arcsight/var/logs/manager/default	Contains troubleshooting information about the Manager
server.std.log	/opt/arcsight/var/logs/manager/default	Contains the stdout output of the Manager
server.status.log	/opt/arcsight/var/logs/manager/default	Contains a dump of all the MBeans, the memory status, thread status, etc.
aggregator.std.log	/opt/arcsight/var/logs/aggregator<service_id>	Contains distributed correlation aggregator output.
correlator.std.log	/opt/arcsight/var/logs/correlator<service_id>	Contains distributed correlation correlator output.
dcache.log	/opt/arcsight/var/logs/dcache<service_id>	Contains distributed correlation distributed cache output.
dcache.std.log	/opt/arcsight/var/logs/dcache<service_id>	Contains distributed correlation distributed cache output.
repo.log	/opt/arcsight/var/logs/repo<service_id>	Contains distributed correlation information repository output.

Log file name	location	Description
repo.std.log	/opt/arcsight/var/logs/repo<service_id>	Contains distributed correlation information repository output.
zookeeper.log	/opt/arcsight/var/logs/mbus/mbus_control<service_id>	Contains message bus ZooKeeper output.
zookeeper.std.log	/opt/arcsight/var/logs/mbus/mbus_control<service_id>	Contains message bus ZooKeeper output.
mbus.log	/opt/arcsight/var/logs/mbus	Contains message bus output.
kafka.log	/opt/arcsight/var/logs/mbus_data<service_id>	Kafka output
kafka.std.log	/opt/arcsight/var/logs/mbus_data<service_id>	Garbage collection output
mbus-configure-instances.log	/opt/arcsight/var/logs/mbus	Contains message bus output.
mbus-configure-instances.std.log	/opt/arcsight/var/logs/mbus	Contains message bus output.
mbussetup.log	/opt/arcsight/var/logs/mbus	Contains message bus output.
Log file for services		
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

Here is what to do if you encounter an unsuccessful installation, or if your installation is corrupted.

For an appliance, restore the factory settings. See Restore Appliance Factory Settings.

For software ESM, 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. After exiting the install process, stop any ArcSight services that are currently running. As user *root*, run the following command:

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

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. For Software ESM, re-install the product.

Customizing the Manager

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

While logged in as user `arcsight`,

1. Stop the Manager if it is running:

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

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

   ```
   ./arcsight managersetup
   ```

3. Follow the prompts on the wizard screens. See the Administrator's Guide for information about specific screens.
4. Restart the Manager and services after the wizard completes by running:

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

Fatal Error when Running the First Boot Wizard - Appliance Installation

This section applies to the appliance installation only.

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.

To resolve this issue, try the following steps:

1. Check the `/opt/arcsight/var/logs/misc/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 are open.
3. If your error occurred before any component got configured, log in as user `root` and do the following:

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

   Rerun the setup using the following commands:

   ```
   cd
   /home/arcsight/install.esm/ESMComponents/service/opt/arcsight/services/bi
   n/scripts
   ```

   ```
   ./esm_setup.sh
   ```

If the above steps do not work, for example, if the setup has already started to configure the Manager or if your installation is corrupted, then restore the factory settings. See Restore Appliance Factory Settings.

Search Query Result Charts Do Not Display in Safari Browser

To enable query results to display as a chart in Safari, you must have the latest version of the Adobe Flash Player Web Plug-In for MAC OS installed.

Hostname Shown as IPv6 Address in Dashboard

This can occur due to a mismatch between the system hostname, the network configuration, and your environment's name resolution. Review your system's hosts file and DNS configuration, as well as the addresses found in the DNS for the system hostname.

Internet Not Accessible From an IPv6 System

Depending on your system configuration and internet access, you might not be able to access the internet from the links provided within the Console or the ArcSight Command Center if your system is purely IPv6. To access the links, copy them to a system that is IPv4 only, or is dual stack.

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 Java Heap Memory	16 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`

E-mail Notification	Internal SMTP server. If you want to use an External SMTP server,
	1. Stop the Manager by running the following command (as user `arcsight`):
	`/etc/init.d/arcsight_services stop manager`
	2. Run the following command from the `/opt/arcsight/manager/bin` directory and set up the external SMTP server when prompted:
	`./arcsight managersetup`
	3. Start the Manager and services by running (as user `arcsight`):
	`/etc/init.d/arcsight_services start all`

Sensor Asset Auto Creation	`true`
Packages/default content installed	Default system content

Appendix C: Using PKCS

Public-Key Cryptography Standard (PKCS) comprises standards used for reliable and secure public key cryptography. Public Key Cryptography works by encrypting the data at the sender's end and decrypting it at the receiver's end.

ESM supports the use of a PKCS#11 token such as the Common Access Card (CAC) or 90Meter for identity verification and access control. It is used to log into the Manager from a user interface. PKCS#11 is Public-Key Cryptography Standard (PKCS), published by RSA Laboratories which describes it as “a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.”

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

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

PKCS#11

PKCS#11, one of the PKCS standards, is an API defining a generic interface to cryptographic tokens, software tokens and hardware tokens such as hardware security modules and smartcards. A cryptographic token is a security device that is used to authorize the use of the software or hardware, such as the smartcard, Common Access Card (CAC), or 90Meter. The credentials of the authorized user are stored on the hardware itself. ESM 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. Make sure that the vendor’s driver and the PKCS#11 driver DLL are installed on the machine on which you plan to use the PKCS#11 token.

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

You can use a PKCS#11 token regardless of the mode in which the ESM client is running (FIPS 140-2 mode or default mode). However, you must configure the ESM Manager to use

"Password or SSL Authentication" when communicating with clients, which you set up by running the Manager Configuration Wizard. For more information about running the wizard, see the Administrator's Guide.

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

Setting Up to Use a PKCS#11 Provider

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

Install the PKCS#11 Provider's Software

Before you use the PKCS#11 token, make sure that you have installed its software on each client system. That includes the ArcSight Console and any machine with a browser from which you intend to access a web-based interface. Refer to your PKCS#11 provider's documentation on how to install and configure it.

Note: When installing ActivClient software, select the **US Department of Defense configuration**.

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

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

For 90Meter, install SCM_1.2.27_64Bit_S.msi. This comes with the 32-bit library as part of your install, which is required.

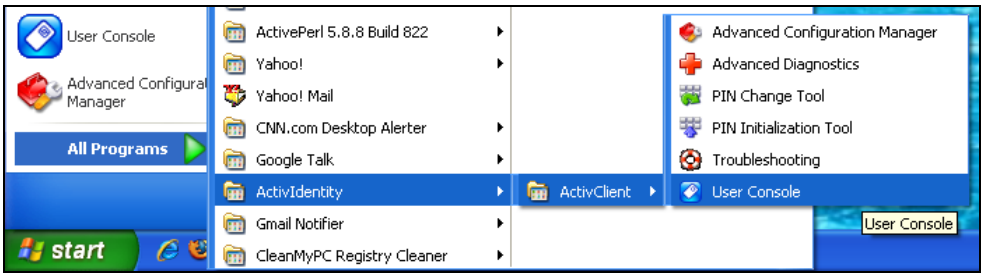
Map a User's External ID to the Subject CN

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

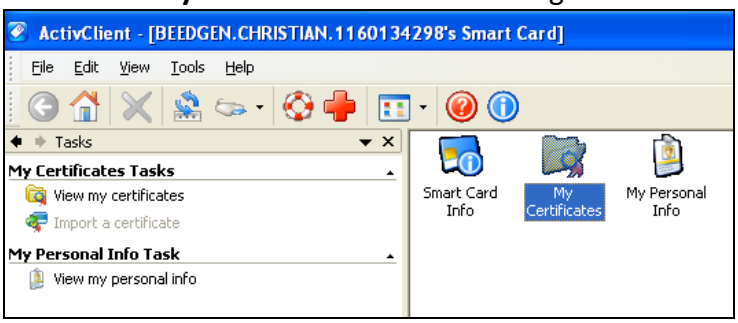
Map the Common Name (CN) on the PKCS#11 token to a User's External ID on the ArcSight Manager. The external user ID must be identical to the Common Name that appears in the PKCS#11 token's ID certificate (include any spaces and periods that appear in the Common name). For example **john.smith.9691998563**.This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

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

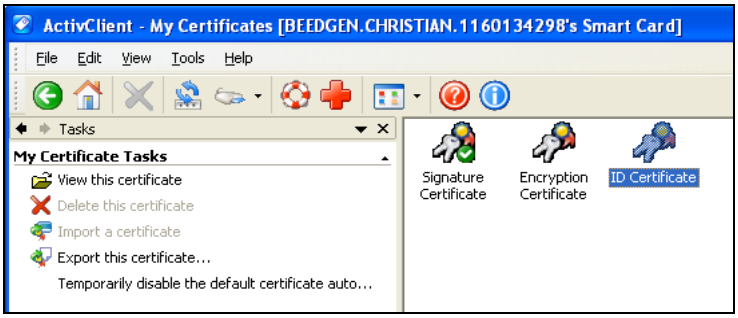
1. Obtain the Subject CN from the CAC/90Meter card.
   a. Insert the CAC/90Meter card into the reader if not already inserted.
   b. Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



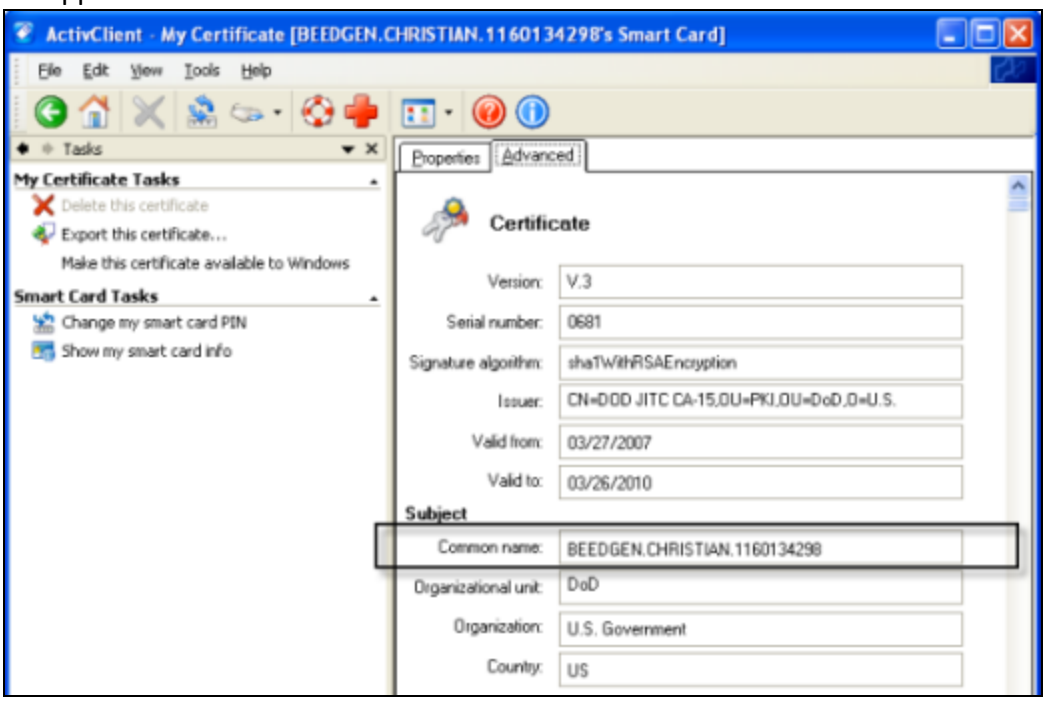
   c. Double-click **My Certificates** in the following screen:



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



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



2. You can make the external ID match the CN in the ArcSight Console:
   a. In the ArcSight Console, go to **Resources > Users > [user group]** and double-click the user whose External ID you want to map to the CAC/90Meter card common name. This opens the Inspect/Edit pane for that user.
   b. Enter the CN you obtained in step 1 into the **External User ID** field and click **Apply**.

Obtain the CAC/90Meter's Issuers' Certificate

PKCS#11 Token authentication is based on SSL client-side authentication. In the case of the Common Access Card, the key pair for the client (the CAC/90Meter device) is stored within the card itself. You need to export the CAC/90Meter's certificate from its keystore so that you can extract the root CA and any intermediate certificates from this certificate.

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

Option 1:

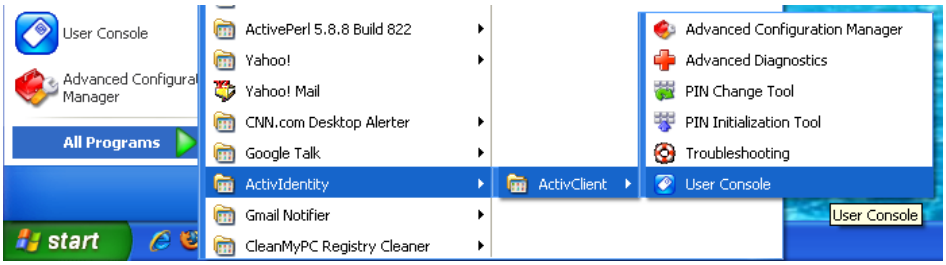
You can obtain the CAC/90Meter card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

Option 2:

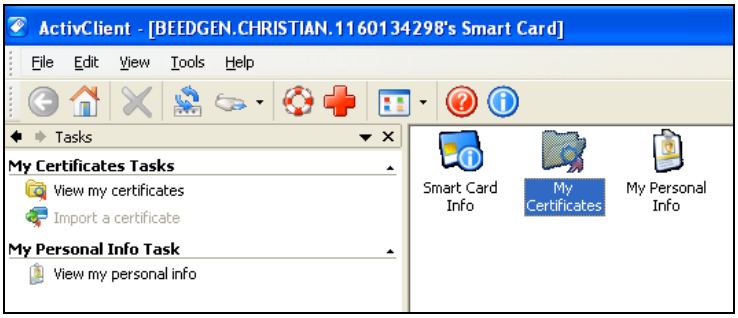
You can export the CAC/90Meter card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

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

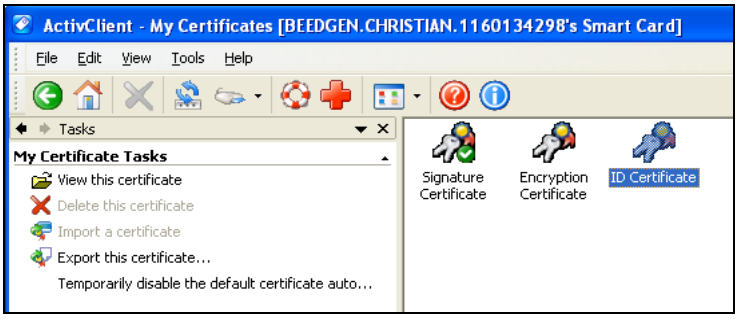
1. Insert the CAC/90Meter card into the reader if not already inserted.
2. Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



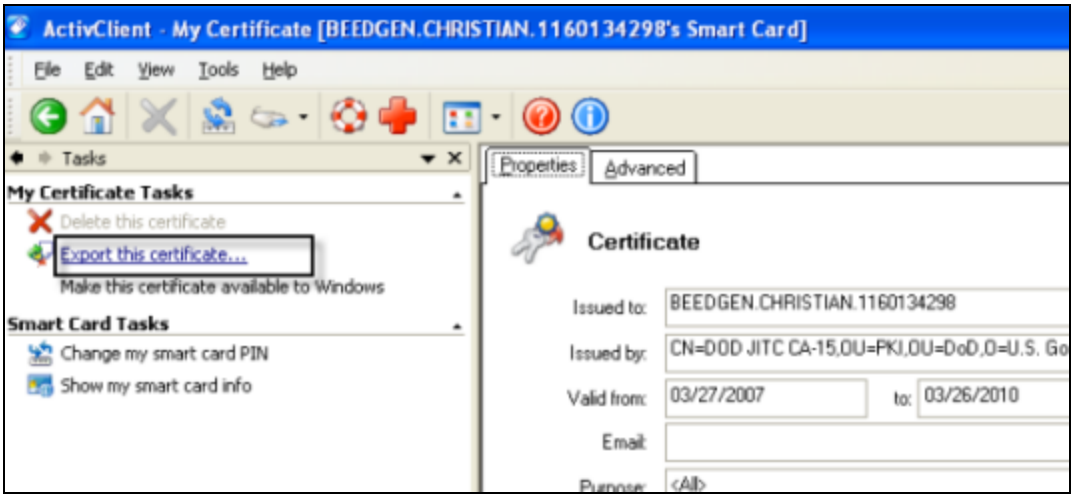
3. Double-click **My Certificates** in the following screen:



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



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



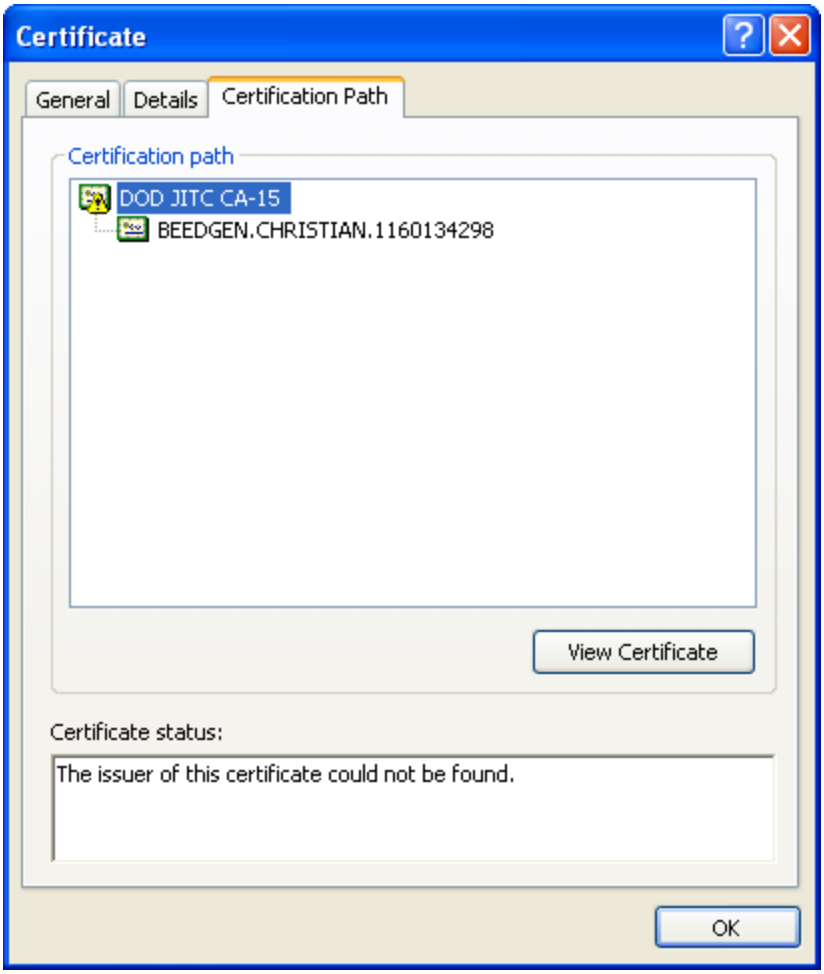
6. Enter a name for the certificate in the **File name** box and navigate to a location on your machine where you want to export it to and click **Save**.
7. When you see the success message, click OK.
8. Exit the ActivClient window.

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

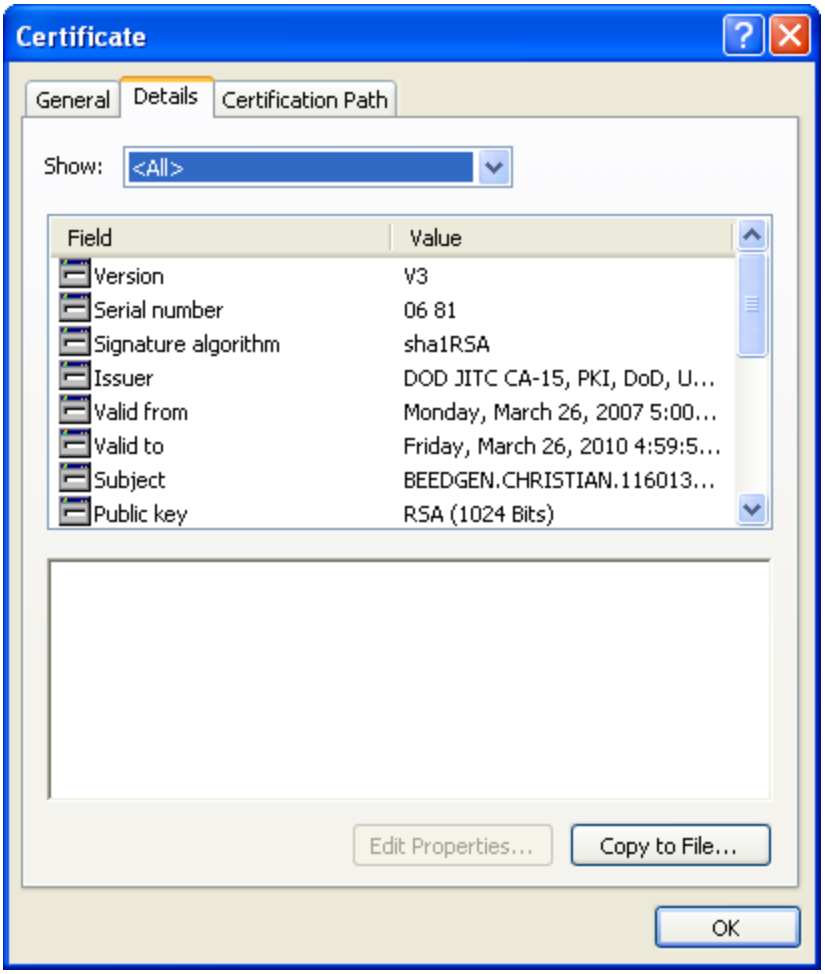
The CAC/90Meter certificate signer's CA root certificate and any intermediate signers' certificate(s) have to be imported into the ArcSight Manager's `keystore`.

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

1. Double-click the certificate that you exported. The Certificate interface opens.
2. Click the **Certification Path** tab and select the root certificate as shown in the example below:



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



5. The Certificate Export Wizard opens. Follow the prompts in the wizard screens and accept all the defaults.
6. Enter a name for the CAC/90Meter root CA certificate file when prompted and continue with the wizard by accepting all the defaults. The certificate is exported to the same location as the CAC/90Meter certificate from which you extracted it.
7. Exit the Certificate dialog.

Import the CAC/90Meter Root CA Certificate into the ArcSight Manager

Import into the ArcSight Manager's Truststore

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

1. If the ArcSight Manager is running, log in as user `arcsight` and use this command:

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

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

   ```
   cd <ARCSIGHT_HOME>
   ```

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store managercerts -
   importcert -alias admin -file admin.cer
   ```

3. Restart the Manager and services while logged in as user *arcsight* :

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

Select Authentication Option in ArcSight Console Setup

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

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

   ```
   ./arcsight consolesetup
   ```

3. Follow the prompts in the wizard screens by accepting all the defaults until you see the screen for the authentication option. The choices are:
   - Password Based Authentication
   - Password Based and SSL Client Based Authentication
   - Password Based or SSL Client Based Authentication
   - SSL Client Only Authentication
4. Select the option for **Password or SSL Client Based Authentication**. You should also have chosen that option when you set up the ArcSight Manager.
5. Follow the prompts in the next few screens by accepting the defaults.
6. On the **Select client keystore type** screen select the **PKCS#11 Token** option.
7. Enter the path or browse to the PKCS#11 library when prompted.

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

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

On 32-bit Windows:
`C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`
On 64-bit Windows:
`C:\Program Files\ActivIdentity\ActivClient\acpkcs211.dll`
(this is the 32-bit version of the ActivClient library)

Or, for ActivClient 7.1 and later:

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

For 90Meter, always use the 32-bit library:
`C:\Program Files\90meter\CACPIVMD\pkcs11\x86\LitPKCS11.dll`

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

Logging in to the ArcSight Console Using PKCS#11 Token

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

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

- Username and password combination (For this option, disconnect the CAC/90Meter card.)
- PKCS#11 Login

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

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

Use a supported web browser to connect to the ArcSight Command Center.

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

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

   a. Open **Tools > Options** and go to the **Advanced > Certificates** tab.
   b. In **Security Devices** -select **Add a new module**.
   c. For "ActiveIdentity" specify 32-bit dll by pointing to
   `C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`

Or, for ActivClient 7.1 and later:

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

For 90Meter everything is configured automatically.

d. Use the **Log In** button to login to the module and enter the PIN when asked. Be sure to use the **Log Out** button to prevent auto-authentication.

e. Restart Firefox and now you can log in to the ArcSight Command Center without any credentials.

3. You will be requested to enter your PIN.

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

4. At the ArcSight Command Center login, *do not* enter any user ID or password. Leave them both blank and click **Login**. User authentication is resolved after you enter the PKCS#11 PIN in the dialog that appears next.

5. Enter your PIN in the Confirmation dialog. The dialog's title and appearance varies, depending on the PKCS#11 token configuration.

Appendix D: Installing ESM in FIPS Mode

ESM supports the Federal Information Processing Standard 140-2 (FIPS 140-2) and Suite B. Once you have configured an ESM system for a particular FIPS mode, you cannot reconfigure that system to enable another FIPS mode. For example, a system configured to enable FIPS 140-2 cannot be reconfigured to enable FIPS Suite B.

Note: FIPS 140-2 mode is the default selection.

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

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

What is FIPS?

FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. A cryptographic module is either a piece of hardware or a software or a combination of the two which is used to implement cryptographic logic. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet the FIPS 140-2 standard. For FIPS compliance, ESM uses Bouncy Castle Java cryptography as the cryptographic module.

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

For FIPS compliance, ESM uses Bouncy Castle Java cryptography, which replaces Mozilla Network Security Services (NSS). Bouncy Castle enables support of TLS 1.2 in FIPS mode as well as in Default mode.

What is Suite B?

Suite B is a set of cryptographic algorithms put forth by the National Security Agency (NSA) as part of the national cryptographic technology. While FIPS 140-2 supports sensitive but unclassified information, FIPS with Suite B supports both unclassified information and most classified to top secret information. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

Note:

- Not all ESM versions support the FIPS with Suite B mode. See the *Technical Requirements* on the ESM documentation page for supported platforms for FIPS with Suite B mode.
- When the Manager is installed in FIPS with Suite B compliant mode, all components (ArcSight Console, SmartConnectors, and Logger, if applicable) must be installed in FIPS with Suite B compliant mode, and the browser used to access ESM must have TLS enabled (SSL protocols are not supported). For information about configuring your browser to support TLS, see Completing Post-Installation Tasks.
- Before installing ESM in FIPS with Suite B mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled ArcSight Manager.

For FIPS cipher suite information, see Choosing between FIPS Mode or Default Mode.

Transport Layer Security (TLS) Configuration Concepts

TLS configuration involves either server side authentication only or both server side and client side authentication. Setting up client side authentication is optional.

For TLS version support information and configuring ESM in FIPS mode, see TLS Support .

Since TLS is based on SSL 3.0, we recommend that you have a good understanding of how SSL works. For more information, see the Administrator's Guide.

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

For information about upgrading an existing default mode installation to FIPS mode, see the Administrator’s Guide.

TLS Support

The version of TLS you must implement depends on ESM/Logger peering, FIPS or non-FIPS implementation, or use of standalone ESM configurations.

Note that:

- For compliance with the Payment Card Industry Data Security Standard (PCI DSS) 3.2, use TLS 1.2. This requires ESM peers to also be running ESM 6.11.0 or later, and Logger peers to be running Logger 6.4 or later
- If you are running a standalone ESM implementation (no peering with other Managers or Logger), use TLS 1.2 for FIPS or non-FIPS configurations.
- For ESM releases prior to ESM 6.11.0 and ESM 7.0.0.1, instances of ESM/Logger that are peering must use TLS 1.0 or TLS 1.1 . Note that use of TLS 1.0 means these systems are not PCI DSS 3.2 compliant.
- For ESM releases prior to ESM 6.11.0 and ESM 7.0.0.1, instances of ESM/Logger that are standalone (non-peering) must use TLS 1.1.
- As of ESM 6.11.0, TLS 1.0, 1.1, and 1.2 are all supported for ESM in FIPS and default (non-FIPS) modes. The SSL protocols are no longer supported.

Also, the following matrix clarifies TLS support for ESM 7.0.0.1 systems that are peering with ESM or Logger:

Version	Non-FIPS	FIPS
ESM 7.3	TLS 1.2	TLS 1.2
ESM 6.11.0 to ESM 7.2.1	TLS 1.0*, TLS 1.1, TLS 1.2	TLS 1.0*, TLS 1.1, TLS 1.2
ESM releases prior to ESM 6.11.0	TLS 1.0*, TLS 1.1	TLS 1.0*, TLS 1.1
Logger 6.4	TLS 1.2	TLS 1.2
Logger releases prior to Logger 6.4	TLS 1.0*, TLS 1.1, TLS 1.2	TLS 1.0*, TLS 1.1
*Note that the use of TLS 1.0 is does not comply with PCI DSS 3.2.		

Server Side Authentication

The first step in an SSL handshake is when the server (ArcSight Manager) authenticates itself to the ArcSight Console. This is called server side authentication.

To set up TLS configuration on your ArcSight Manager for server side authentication, you need:

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

Next, you should export the ArcSight Manager's certificate from its keystore and lastly import this certificate into the keystore of the clients that will be connecting to this ArcSight Manager.

Client Side Authentication

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

For the client to authenticate itself to the ArcSight Manager, you should have the following in the client's keystore:

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

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

For detailed procedures on each of the steps mentioned above, see the information about establising SSL client authentication in the Administrator's Guide.

Exporting the Manager's Certificate to Clients

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

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

```
./arcsight keytool -exportcert -store managerkeys -alias mykey -file <path_
to_manager_certificate.cer>
```

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

For example, to export the ArcSight Manager's certificate to the`/opt/arcsight/manager` directory, run:

```
./arcsight keytool -exportcert -store managerkeys -alias mykey -file
manager.cer
```

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

Many utility functions for the Manager (for example, `arcsight archive` or `arcsight managerinventory`) are clients for the Manager. In FIPS mode, the Manager certificate is not automatically imported. In order to use the utilities, import the certificate by running:

```
./arcsight keytool -importcert -store clientcerts -alias <hostname> -file
<path_to_manager_certificate.cer>
```

Using PKCS#11 Token With a FIPS Mode Setup

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

Installing the ArcSight Console in FIPS Mode

Note: If you would like to set up client-side authentication on the ArcSight Console, see the Administrator's Guide.

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

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

Refer to the ESM Product Lifecycle document available on the Micro Focus Community for details on supported platforms for the ArcSight Console.

This section tells you how to install the ArcSight Console in FIPS mode only. For details on installing the ArcSight Console in default mode, see Installing the Console .

In order for an ArcSight Console to communicate with a FIPS enabled ArcSight Manager, the ArcSight Console must trust the ArcSight Manager. This trust is established by importing the ArcSight Manager's certificate into the ArcSight Console's keystore. After you configure the ArcSight Console for FIPS, it will automatically import the ArcSight Manager's certificate the first time you start it. Note that if there is a certificate resident in the keystore, no import will occur.

To install the ArcSight Console in FIPS mode:

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

   Select **Run console in FIPS mode** and click **Next**.
5. You will be reminded that once you select the FIPS mode, you will not be able to revert to the default mode. Click **Yes**.
6. You will be prompted to select a cipher suite. Select the type of FIPS the ArcSight Manager uses and click **Next**.
7. Next you will be prompted for the ArcSight Manager’s hostname and port. The ArcSight Manager hostname must be the same (short name, fully qualified domain name, or IP address) as the Common Name (CN) you used when you created the ArcSight Manager key pair.
8. Follow the prompts in the next few wizard screens until you get to the screen where you have to select the authentication option. For information about specific screens, see Installing the Console .

   Select **Password Based or SSL Client Based Authentication**, which also must be the option that you had set on the ArcSight Manager when installing it.
9. If you are using SSL client-based authentication and if you plan to use a PKCS#11 token with the ArcSight Console, select **PKCS#11 Token** option in the following screen. If you are using different authentication, you do not see this screen and you can skip this step.

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

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

   On 64-bit Windows:
   `C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`

   Or, for ActivClient 7.1 and later, also on 64-bit Windows:

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

   These are both the 32-bit version of the ActivClient library.

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

   Alternatively, 90Meter is available at:

   `C:\Program Files\90meter\CACPIVMD\pkcs11\x86\litpkcs11.dll`

   After completing the Configuration Wizard, follow the procedure about setting up client-side authentication in the Administrator’s Guide.

10. Follow the prompts in the next few wizard screens to complete the ArcSight Console installation. For information about specific screens, see Installing the Console .

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

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

You can connect a default mode Console to a FIPS 140-2 Manager with no additional configuration.

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

Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers

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

If you need to import an ArcSight Manager's certificate into the ArcSight Console's keystore manually, see the Administrator's Guide.

Installing SmartConnectors in FIPS Mode

When the ArcSight Manager is installed in FIPS mode, the SmartConnectors must also be installed in FIPS mode. When you run the SmartConnector installation, (see the SmartConnector documentation) select **Enable FIPS Mode**. Then continue until you see the screen that offers you the choice to Continue or Exit. Select **Exit** and click **Next**. On the next screen, click **Done**. You have to import the ArcSight Manager's certificate to allow the connector to trust the ArcSight Manager before adding a new connector. See the SmartConnector documentation for the specific SmartConnector you are installing for details. Also, for details on FIPS mode settings for SmartConnectors, see Configuring FIPS and Non-FIPS Compliant Modes for ESM and SmartConnectors, available on Micro Focus Community .

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

- For Linux: cd <CONNECTOR_HOME>/current/jre/bin> and then run:

```
./keytool -J-Djava.security.egd=file:/dev/urandom -importcert -file
<certificate path> -keystore <CONNECTOR_
HOME>/current/user/agent/fips/bcfips_ks -storepass changeit -storetype
BCFKS -providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
<CONNECTOR_HOME>/current/lib/agent/fips/bc-fips-1.0.0.jar -alias "myalias"
```

- For WIN 64-Bit: cd <CONNECTOR_HOME>\current\jre\bin> and then run:

```
keytool -importcert -file <CONNECTOR_HOME>\current\manager.cert -keystore
<CONNECTOR_HOME>\current\user\agent\fips\bcfips_ks -storepass changeit -
storetype BCFKS -providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
<CONNECTOR_HOME>\current\lib\agent\fips\bc-fips-1.0.0.jar -alias "myalias"
```

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

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

1. Select **Add a Connector** and press **Enter**.
2. Select the connector to configure and press **Enter** to continue.
3. For each of the parameters you are shown next, you can either change the value or accept the default value. Continue until you get to the Type of Destination parameters.
4. Select **ArcSight Manager (encrypted)** as the type of destination and press **Enter**.
5. Under **Destination Parameters**, or each of the parameters you are shown next, you can either change the value or accept the default value. When you get to them, enter the Manager Hostname and login credentials.
6. For the **FIPS Cipher Suites parameter**, choose from:
   - **FIPS Default**
   - **FIPS with Suite B 128 bits**
   - **FIPS with Suite B 192 bit**

   Press **Enter** to continue.
7. Enter the connector details such as the name and location, which can be any values you want.
8. Decide whether to install the connector as a service or leave it as a standalone application

and press **Enter** to Continue.

9. Exit the connector configuration wizard.

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

How Do I Know if My Installation is FIPS Enabled?

To verify whether your existing installation has been installed in FIPS mode or default mode, check the `fips.enabled` property in the `<ARCSIGHT_HOME>/config/esm.properties` file on the Manager and the `<ARCSIGHT_HOME>/config/console.properties` file for the ArcSight Console.

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

Also, when the Console starts in FIPS mode, there is a message indicating that in `console.log`; when a Manager starts in FIPS mode there is a message to that effect in `server.std.log`.

Appendix E: Transformation Hub Best Practices

This appendix contains best practices for using Transformation Hub with ESM. For information about configuration and property settings for Transformation Hub, see the Administrator's Guide for the ArcSight Platform.

- Use host names and *not* IP addresses to connect to Transformation Hub.
- Create a separate topic on Transformation Hub for connectors to use. Connectors can write binary events to this topic and ESM can consume events from this topic. Configure the topic with a minimum of 5 partitions. ESM automatically adjusts the number of consumers from ESM to match the number of partitions. For more information, see the Administrator's Guide for the ArcSight Platform.
- Do not send both binary and CEF events to the same topic. Always use a dedicated topic on Transformation Hub for each type of event.
- When configuring the retention policy settings for time and space retention on Transformation Hub, consider the amount of data that you expect ESM to consume. If the amount of data in a topic is more than ESM can consume before the Transformation Hub retention policy activates, the portion of the topic that ESM has not read might be deleted. For information about configuring the retention policy on Transformation Hub, see the Administrator's Guide for the ArcSight Platform.
- Certificates that are used with Transformation Hub (for both TLS and client authentication) are read once during ESM startup. To add or change certificates after ESM starts, make the changes and then restart ESM.
- Either start Transformation Hub and configure ESM's binary topic before you start ESM, or configure the topic soon after starting ESM. When you start ESM after you configure it to use Transformation Hub, ESM will try to connect to Transformation Hub every few minutes using the configuration and certificates that were read at ESM startup. If the connection is not successful after four hours, ESM assumes that Transformation Hub will not be available in the near future and only attempts to connect every two hours.

Appendix F: Locales and Encodings

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, time zone settings, and Daylight Saving Time setting for that country or language. This document describes the updates to be taken into consideration when configuring ESM for a supported language.

Locale and Encoding Terminology

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.

Region Code

Currently, the region code standard that is used is **ISO 3166-2**. Previous versions of ESM used the **FIPS 10-4** region-code standard, which is no longer supported. As a result, there is a change in the way region is represented in the geographical information for IP Addresses. For example, ESM 6.9.1 and earlier would report 54 as the region code for the IP address 176.62.127.255. In later releases, it is reported as OMS.

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 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 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

If your connector receives logs that contain timestamps or date formats in a non-English language or locale (for example, "mai 24, 2015 12:56:07.615" where "mai" is German for May), configure the `agent.parser.locale.name` property in the `agent.properties` file. This file is located in the `<ARCSIGHT_HOME>/current/user/agent` directory.

Set the `agent.parser.locale.name` property to the value that corresponds to the Connector's locale. By default, this property is set to en_US. Refer to the table in List of Possible Values for possible values for this property.

List of Possible Values

`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	
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		

Values	Language	Country	Variant
ca_ES	Catalan	Spain	
cs	Czech		
cs_CZ	Czech	Czech Republic	
da	Danish		
da_DK	Danish	Denmark	
de	German		
de_AT	German	Austria	
de_CH	German	Switzerland	
de_DE	German	Germany	
de_LU	German	Luxembourg	
el	Greek		
el_GR	Greek	Greece	
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	

Values	Language	Country	Variant
es_CL	Spanish	Chile	
es_CO	Spanish	Columbia	
es_CR	Spanish	Costa Rica	
es_DO	Spanish	Dominican Republic	
es_EC	Spanish	Ecuador	
es_ES	Spanish	Spain	
es_GT	Spanish	Guatemala	
es_HN	Spanish	Honduras	
es_MX	Spanish	Mexico	
es_NI	Spanish	Nicaragua	
es_PA	Spanish	Panama	
es_PE	Spanish	Peru	
es_PR	Spanish	Puerto Rico	
es_PY	Spanish	Paraguay	
es_SV	Spanish	El Salvador	
es_UY	Spanish	Uruguay	
es_VE	Spanish	Venezuela	
et	Estonian		
et_EE	Estonian	Estonia	
fi	Finnish		
fi_FI	Finnish	Finland	
fr	French		
fr_BE	French	Belgium	

Values	Language	Country	Variant
fr_CA	French	Canada	
fr_CH	French	Switzerland	
fr_FR	French	France	
fr_LU	French	Luxembourg	
hi_IN	Hindi	India	
hr	Croatian		
hr_HR	Croatian	Croatia	
hu	Hungarian		
hu_HU	Hungarian	Hungary	
is	Icelandic		
is_IS	Icelandic	Iceland	
it	Italian		
it_CH	Italian	Switzerland	
it_IT	Italian	Italy	
iw	Hebrew		
iw_IL	Hebrew	Israel	
ja	Japanese		
ja_JP	Japanese	Japan	
ko	Korean		
ko_KR	Korean	Korea	
lt	Lithuanian		
lt_LT	Lithuanian	Lithuania	
lv	Latvian		
lv_LV	Latvian	Latvia	

Values	Language	Country	Variant
mk	Macedonian		
mk_MK	Macedonian	Macedonia	
nl	Dutch		
nl_BE	Dutch	Belgium	
nl_NL	Dutch	Netherlands	
no	Norwegian		
no_NO	Norwegian	Norway	
no_NO_NY	Norwegian	Norway	Nynorsk
pl	Polish		
pl_PL	Polish	Poland	
pt	Portuguese		
pt_BR	Portuguese	Brazil	
pt_PT	Portuguese	Portugal	
ro	Romanian		
ro_RO	Romanian	Romania	
ru	Russian		
ru_RU	Russian	Russia	
sk	Slovak		
sk_SK	Slovak	Slovakia	
sl	Slovanian		
sl_SI	Slovanian	Slovania	
sq	Albanian		
sq_AL	Albanian	Albania	
sv	Swedish		

Values	Language	Country	Variant
sv_SE	Swedish	Sweden	
th	Thai		
th_TH	Thai	Thailand	
th_TH_TH	Thai	Thailand	TH (Numbers have Thai digits instead of Arabic digits.)
tr	Turkish		
tr_TR	Turkish	Turkey	
uk	Ukranian		
uk_UA	Ukranian	Ukraine	
vi	Vietnamese		
vi_VN	Vietnamese	Vietnam	
zh	Chinese		
zh_CN	Chinese	China	
zh_HK	Chinese	Hong Kong	
zh_TW	Chinese	Taiwan	

Key-Value Parsers for Localized Devices

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

event.destinationUserName=User

...and the received event message is:

User=김

...where 김 is Korean for KIM.

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

If the received event message is:

우새르

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

If you encounter a need for a localized device, please contact Customer Support.

Appendix G: Restore Appliance Factory Settings

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

CAUTION: ***Factory reset irrevocably deletes all event and configuration data.*** Use the following procedure to restore the appliance to its original, factory settings:

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

   System Restore automatically detects and displays the archive image.

   The image is named following this pattern:

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

   where YYYY-MM-DD is the date, <model> is the appliance model, and <build_num> is the build number of the image being restored. If you encounter any issues with the image, contact Customer Support.
4. Press **F10** (VERIFY) to check the archive for damage before performing the restore.
5. Press **F1** (AUTOSELECT) to automatically map the source image.
6. Press **F2** (RESTORE) to begin the restore process.

   CAUTION: Do not interrupt or power-down the appliance during the restore process. Interrupting the restore process may force the system into a state from which it cannot be recovered.
7. When the restore process is completed, press **F12** to reboot the appliance.

Send Documentation Feedback

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

Feedback on Installation Guide (ESM 7.5)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!