
opentext™

ESM Appliance

EC8300 Model

Software Version: 24.4

**Administrator's Guide to Hardware Appliances
for ArcSight ESM**

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 OpenText

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.
Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://www.microfocus.com/en-us/contact-support/stackb
Support Web Site	https://www.microfocus.com/en-us/support
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/#gsc.tab=0

Contents

About this Guide	5
Intended Audience	5
Contact Information	5
Chapter 1: Overview	6
Chapter 2: Setting Up an ESM Appliance	8
Powering On the ESM Appliance	8
Setting Up the Appliance for Remote Access	9
Changing the iDRAC password on your Appliance	9
Firewall	10
Encryption of SEDs	10
Initializing the ESM Appliance	10
First Boot Initialization of the ESM Appliance (Bootstrapping)	11
Regeneration of the First Login Token	14
Keep These TCP Ports Open	14
Configuring the Custom Firewall Zone	15
Planning for a Distributed Correlation Cluster	16
Converting Hierarchical Implementations to a Distributed Correlation Cluster	16
Understanding Cluster Requirements	16
Placing Information Repository Instances on a Separate Partition	17
Understanding Recommended Cluster Configurations	17
Choosing the Preferred IP Protocol	20
Preparing for IPv6 Only Communication	20
Creating the /var/opt/arcsight Directory	21
Starting the Installer	21
Running the Installation File	21
Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard	22
Installing ESM on the Persistor Node	24
Adding Nodes to a Cluster	29
Configuring the Cluster	31
Configuring Certificate Management	32
Adding a Node to the Cluster with Certificate Management	34
Setting Up Key-Based Passwordless SSH - Distributed Correlation Mode Only	37
Appliance Licenses	37
Obtaining Your License	37

Chapter 3: Converting from Compact to Distributed Mode	38
Chapter 4: Restore Procedures	42
Restoring an Appliance to Factory Settings	42
Restoring an Appliance Using a USB Memory Stick	42
Image Burning	42
Restore Procedure:	43
Restoring an Appliance Using iDRAC Access	44
Restore Procedure:	44
Publication Status	46
Send Documentation Feedback	47

About this Guide

This installation guide provides instructions on the following:

- Installing and initializing ESM in distributed mode, using the ESM E8400 and ESM EC8300 appliances.
- Converting a previously installed ESM E8400 appliance from compact mode to distributed mode

For more information, see [How the ESM Appliance Works](#).

Intended Audience

This book provides information for admins who need to install, initialize, and restore ESM appliances.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact [OpenText Customer Care](#).

Chapter 1: Overview

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. EC8300 is the hardware appliance custom built for ESM.

ESM collects, normalizes, aggregates, and filters millions of events from thousands of assets across your network into a manageable stream that is prioritized according to risk, vulnerabilities, and the criticality of the assets involved. These prioritized events can then be correlated, investigated, analyzed, and remediated using ESM tools, giving you situational awareness and real-time incident response time.

- **Correlation**—Many interesting activities are often represented by more than one event. Correlation is a process that discovers the relationships between events, infers the significance of those relationships, prioritizes them, then provides a framework for taking actions.
- **Monitoring**—Once events have been processed and correlated to pinpoint the most critical or potentially dangerous of them, ESM provides a variety of flexible monitoring tools that enable you to investigate and remediate potential threats before they can damage your network.
- **Workflow**—The workflow framework provides a customizable structure of escalation levels to ensure that events of interest are escalated to the right people in the right timeframe. This enables members of your team to do immediate investigations, make informed decisions, and take appropriate and timely action.
- **Analysis**—When events occur that require investigation, ESM provides an array of investigative tools that enable members of your team to drill down into an event to discover its details and connections, and to perform functions, such as NSlookup, Ping, PortInfo, Traceroute, WebSearch, and Whois.
- **Reporting**—Briefing others on the status of your network security is vital to all who have a stake in the health of your network, including IT and security managers, executive management, and regulatory auditors. ESM's reporting and trending tools can be used to create versatile, multi-element reports that can focus on narrow topics or report general system status, either manually or automatically, on a regular schedule.

With distributed correlation you can configure and deploy multiple instances of correlators and aggregators on multiple nodes in a cluster. The multiple instances of correlators and aggregators run as individual services and distribute the correlation workload across these services. You can configure the multiple services to run on several machines, which are the nodes in a distributed correlation cluster.

The benefits of processing on multiple systems in a cluster are higher performance and fault tolerance. The multiple instances of correlators and aggregators support the faster processing of larger numbers of events, depending on your content and environment. Think of the distributed correlation cluster as a large instance of ESM, to which you can add more nodes (and instances of correlators and aggregators) as needed to increase processing power.

For more information about distributed correlation mode, see [Distributed Correlation](#) in [ESM 101](#).



The purpose of this guide is to help you perform the initial configuration of your ESM appliance, so that you can start taking advantage of all its features. For more information on the usage and settings of specific features, please refer to the [ArcSight Command Center User's Guide for ArcSight ESM 24.3](#) and the [ArcSight Console User's Guide for ArcSight ESM 24.3](#).

Chapter 2: Setting Up an ESM Appliance

This section describes how to rack mount your ESM EC8300. These basic steps enable you to start using your ESM appliances.

	Task	See
<input type="checkbox"/>	1. Power on the Appliance	Powering On the ESM Appliance
<input type="checkbox"/>	2. Set up Remote Access	"Setting Up the Appliance for Remote Access" on the next page
<input type="checkbox"/>	3. (Optional) Encryption of SEDs	"Encryption of SEDs" on page 10
<input type="checkbox"/>	4. Appliance Initialization Procedures	"Initializing the ESM Appliance " on page 10
<input type="checkbox"/>	5. Open the appropriate ports	"Keep These TCP Ports Open" on page 14
<input type="checkbox"/>	6. Configure the custom firewall	"Configuring the Custom Firewall Zone" on page 15
<input type="checkbox"/>	7. Prepare for a distributed correlation cluster	"Planning for a Distributed Correlation Cluster" on page 16
<input type="checkbox"/>	8. Create the /var/opt/arcsight directory	"Creating the /var/opt/arcsight Directory" on page 21
<input type="checkbox"/>	9. Appliance Licenses	"Appliance Licenses" on page 37

Powering On the ESM Appliance

Before you Begin:

Redeem your license key by following the instructions in the documents you received when purchasing. Redeeming this key gets you the license that you need to access the ESM functionality.

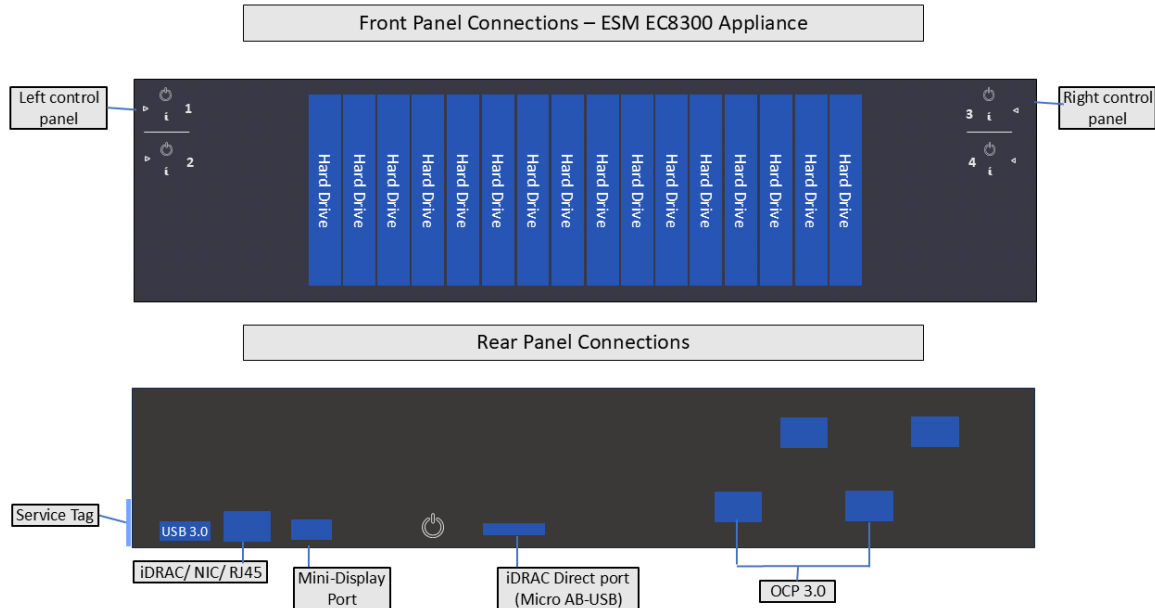
To install the appliance:

1. Unpack the appliance and its accompanying accessories.



Note: Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.
3. Make the front and rear panel connections. The diagram below offers a general view of the basic connections:



4. To enable local access to the Appliance, connect a keyboard, monitor, and mouse to the Appliance ports.
5. Power on the appliance.

Setting Up the Appliance for Remote Access

All appliances are equipped with an iDRAC Service Module (iSM) for remote access. OpenText strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you or Customer Support (with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and control over the powering on and off of the box.

Changing the iDRAC password on your Appliance

Appliance boxes come with a random iDRAC password. For information on how to locate the password, see [Secure Default Password](#).


This is a unique password, which will be required the first time iDRAC is accessed. The appliance then will prompt for a new password to be chosen. For security reasons, OpenText recommends to change this password as soon as possible.

To set up your appliance for remote access, follow the instructions in the [EMC iDRAC Service Module](#).

Firewall

The firewall for the ESM appliance comes pre-configured, with the following TCP ports open by default to facilitate the initial setup:

Port	Description
22	Used by the appliance installer
7443	Used by the appliance installer
8443	SmartConnectors and consoles
9000	Peering

 **Note:** If you do not plan to use peering in your environment, disable port 9000.

Encryption of SEDs

The ESM Appliances support FIPS enabled self-encrypting disks (SEDs).

A SED is a data storage device with built-in cryptographic processing to encrypt and decrypt the data it contains. This process occurs within the device itself, independent of any connected information system, and it provides data protection against the loss or theft of the disks, as well as certain levels of hacking attempts.

This protection consists of setting up passphrase-access-only.

The SEDs ship without the passphrase, allowing you to chose your own. To set up a passphrase, first follow the steps to establish a [security key](#).

The chosen passphrase can then be applied to pre-existing virtual disks by following the steps in [Secure a pre-existing virtual disk](#).

To change or disable a security key, please follow the specific procedures listed under [this section](#).

Initializing the ESM Appliance

The initialization of a ESM appliance consists of two parts: the first boot (bootstrapping) of the process through the console, and the installation of the software.

First Boot Initialization of the ESM Appliance (Bootstrapping)



Tip: Be aware that this process will require network information for the appliance, such as:

- Static IP address
- Resolvable FQDN hostname
- NTP server that's both accessible and running

All of this information must be available to successfully complete the bootstrapping.

1. Log into your appliance using iDRAC (see "[Setting Up the Appliance for Remote Access](#)" on [page 9](#) for instructions), and launch the Virtual Console.
2. Turn on the appliance using the Power Controls option, in case the appliance is off.
3. Using the local drive (NVMe), select from the menu the version of Red Hat you want to boot from.
4. From the console, login using your default username (otadmin) and password (change_me).
5. Once the default credentials are entered, you will be asked to change the password for otadmin:

```
You are required to change your password immediately (administrator enforced).
```

```
Current password:
```

```
New password:
```

```
Retype new password:
```




Note: The STIG-compliant password policy rules for both the arcsight and the root password require:

- A minimum of 15 characters
- A minimum of 1 number
- A minimum of 1 lowercase character
- A minimum of 1 uppercase character
- A minimum of 1 special character
- A maximum of 2 consecutive repeating characters
- A maximum of 4 consecutive repeating characters of the same class
- A minimum of 8 different characters
- To not be a word from the dictionary
- To be different from the last seven passwords

- The **OpenText Appliance** splash screen will appear, with the **User must set 'root' password to proceed** message. You will be required to enter the otadmin user password you just reset to make the change to the root password:

```
password for otadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

 Once your passwords have been set, you will need to wait for at least one day to update to a different one. And the maximum expiration period for a password is 60 days.

- Set the arcsight user password.

```
password for arcsight
Changing password for user arcsight.
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

- Complete the **Network Configuration**. The screen will display a list of network interfaces and their status:

```
*****
Network Configuration
*****
WARNING: You must specify static IP address and resolvable hostname
(FQDN).
*****
List of network interfaces
*****
enoxxxxnp0      UP           xx:xx:xx:xx:xx:xx      <BROADCAST, MULTICAST, UP, LOWER
enoxxxx        DOWN        xx:xx:xx:xx:xx:xx      <NO-CARRIER, BROADCAST, , MULTI
ensxxx         DOWN        xx:xx:xx:xx:xx:xx      <NO-CARRIER, BROADCAST, MULTICA
ensxxx         DOWN        xx:xx:xx:xx:xx:xx      <NO-CARRIER, BROADCAST, MULTICA
*****
Select one active connection to configure:
*****
1) enoxxxxnp0
#? 1
```

Select the number of the active connection you want to configure.

- Configure the network using an IPv4 address by providing this information:

```

*****
Configure the network connection enoxxxxnp0 for device enoxxxxnp0:
*****
Hostname: your_appliance_host_fqdn

What type of Networking do you want to setup? 1. IPv4

IP Address:
Netmask [1-31]:
Default Gateway:
Primary DNS server:
Secondary DNS server (optional):
DNS Search Domains: your_appliance_domain
    
```

10. (Optional) Enter the date and time information.

11. Configure the NTP server.

```

(one entry per line, press enter when done)
NPT Servers:
    
```

Once all this information has been provided, the console will display a summary of the network configuration and NTP server configuration, and will ask you to verify by entering y:

```

Do you want to apply this configuration? (y/n)
    
```

If you need to correct the information, enter n, and the process will ask you for each item again. If you enter y, the process will continue:

```

Generate self-signed certificate and first time login token...
    
```

12. If the configuration ends successfully, you will see the following message:

```

*****
The appliance network and NTP server have been setup successfully
*****
Go to https://<your_appliance_host_fqdn>:7443 to install ESM product
IMPORTANT: You will need the token to login for the first time:
XXXXXXXXXX
*****
    
```



Note: The message to go to <your_appliance_host_fqdn>:7443 to install ESM does not apply to distributed mode. Proceed to the next part of the process.



The console will not allow you to copy the token, which you will need for your first login to the **ESM Installer Web App**. Access the URL provided above in your browser, and type the token manually as shown in the console.

Regeneration of the First Login Token

If you need to obtain a First Login Token again (other than with the preceding procedure), you can regenerate it by running the following command as the otadmin user in the console:

```
/var/opt/appliance/appliance_scripts/generate_first_login_token.sh
```

The command output should appear as follows:

```
=====
Go to https://<your_appliance_host_fqdn>:7443 to install ESM product
IMPORTANT: You will need the token to login for the first time:
XXXXXXXXXX
=====
```

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. For more information, see ["Configuring the Custom Firewall Zone" on the next page](#).

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 [ESM Administrator's Guide](#).

Configuring the Custom Firewall Zone

The custom firewall zone secures the communication between the distributed cluster services, restricting inbound and outbound communication between nodes in the custom zone. If a host from outside the custom zone attempts to access a specific port, the connection will be denied.

Run the following commands as user `otadmin` on all the nodes in the cluster:

1. Create a new custom firewall zone.

```
sudo firewall-cmd --permanent --new-zone=<my-esm-zone-name>
```

2. Add cluster node IP addresses to the custom zone.

```
sudo firewall-cmd --permanent --zone=<my-esm-zone-name> --add-source=<cluster_node_ip>
```



Note: Execute this command for each cluster node IP address (excluding the current node) you want to add to the custom zone `<my-esm-zone-name>`. Replace `<cluster_node_ip>` with the IP address of the node you want to add.

3. Open information repository ports in the custom zone.

```
sudo firewall-cmd --permanent --zone=<my-esm-zone-name> --add-port=3179-3182/tcp
```

4. Open ports for other distributed services (such as aggregators, correlators, and mbus) in the custom zone.

```
sudo firewall-cmd --permanent --zone=<my-esm-zone-name> --add-port=10000-10100/tcp
```

5. Enable SSH service for SSH communication between nodes in the custom zone.

```
sudo firewall-cmd --zone=<my-esm-zone-name> --add-service=ssh --permanent
```

6. Reload firewall configuration.

```
sudo firewall-cmd --reload
```

7. Verify the custom zone firewall configuration.

```
sudo firewall-cmd --list-all --zone=<my-esm-zone-name>
```

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.



Note: In your distributed environment, use the E8400 appliance for the persistor node. Use the EC8300 appliance for the non-persistor nodes.

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), Open Text 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 have `/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 creates `/var/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.

To create the `/var/opt/arcsight` directory, see ["Creating the /var/opt/arcsight Directory" on page 21](#).

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, Open Text 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.

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

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

Open Text 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 [ESM 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. Open Text recommends keeping the 127.0.0.1 (localhost - lo0) 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.

Creating the /var/opt/arcsight Directory

You must create the /var/opt/arcsight directory on all cluster nodes before installing ESM. For more information, see the "Placing Information Repository Instances on a Separate Partition" section in ["Planning for a Distributed Correlation Cluster" on page 16](#).

To create the /var/opt/arcsight directory:

1. Log in as user otadmin.
2. Run the following commands on all cluster nodes:

```
sudo mkdir -p /var/opt/arcsight
```

```
sudo chown arcsight:arcsight /var/opt/arcsight
```


Starting the Installer

Before you run the installer, you must prepare the system for ESM installation in all nodes of the cluster.

To prepare the system and run the installer:

1. Log in as user otadmin.
2. Run the following script:


```
sudo /var/opt/appliance/install.esm/Tools/prepare_system.sh
```

 **Note:** A reboot is not necessary.

3. Log in as user arcsight.
4. Run the following script:

```
/var/opt/appliance/install.esm/ArcSightESMSuite.bin -i console
```

The installation begins.

 **Note:** 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. (Conditional) If you see a Platform Environmental Issue message, type **2** and then press **Enter**.
2. Read the **Introduction** message and press **Enter**.
3. On the **License Agreement** panel, press **Enter** to page through the agreement. If you accept the License Agreement, type **y** and press **Enter**.
4. Read the **Special Notice** and press **Enter**.
5. 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**.
6. Review the **Pre-Installation Summary**. Press **Enter** to continue.
Under **Installing** a progress bar appears.

The Suite Installer installs each component.

After the components are installed it says **Installation Complete**. Press **Enter** to exit the installer.

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 [ESM Administrator's Guide](#).

When you install ESM in distributed correlation mode, you must first [install ESM on the persistor node](#) (E8400). After you install ESM on the persistor node, [install it on the other cluster nodes](#) (EC8300) as needed and then [perform post-installation configuration tasks](#).

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.

Following is a summary of the installation process:

1. [Install ESM on the persistor node](#).



Note: To run the `setup_services` script after first boot setup, log in as user `otadmin`.

2. Verify that the information repository is available on the persistor node:

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

3. [Add nodes to the cluster.](#)

4. (Conditional) If you did not add correlators and aggregators during the first boot setup of the non-persistor nodes, add aggregators and correlators on the non-persistor nodes:

```
/opt/arcsight/manager/bin/arcsight correlationsetup
```

5. (Conditional) if you did not configure the dcache instances during the first boot setup of the persistor and non-persistor nodes, add dcache instances on the persistor and non-persistor nodes:

```
/opt/arcsight/manager/bin/arcsight dcachesetup
```

6. On the persistor node (for more information about the following tasks, see [Configuring the Cluster](#)):

- a. Configure passwordless SSH:

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

- b. Approve all certificates:

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

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

- c. Stop all services and start the information repository:

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

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

- d. Configure message bus data and message bus control instances:

```
/opt/arcsight/manager/bin/arcsight mbussetup
```



Note: For the recommended distribution of services, see [Planning for a Distributed Correlation Cluster](#).

- e. (Conditional) Configure additional information repository instances:

```
/opt/arcsight/manager/bin/arcsight repositup
```



Note: For the recommended distribution of resources, see [Planning for a Distributed Correlation Cluster](#).

- f. Start all services and verify their status:

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

Installing ESM on the Persistor Node



Note: This section applies to setting up distributed mode in a fresh installation. If you already have an E8400 appliance set up in compact mode and need to convert to distributed mode, see ["Converting from Compact to Distributed Mode" on page 38.](#)

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, Open Text 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. Open Text 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. Start the configuration wizard:

```
/opt/arc_sight/manager/bin/arc_sight 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.



Note: Keep track of the password you specify. It will be required during the "[Configuring the Cluster](#)" on [page 31](#) section and whenever you add new nodes the cluster in the future.

For information about password restrictions, see the [ESM 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 [ESM 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 [ESM 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.



Note: If you are using a demo license, enter 0.

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 [ESM 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 [ESM 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 [ESM 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 7.8 requires Recon 1.5.1.

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[®] IT Service Management \(ITSM\)](#).

- 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 [ESM Administrator's Guide](#).
22. To set up the services, log in as user otadmin and run the following script:

```
sudo /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. Open Text 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.



Note: If you have Certificate Management enabled, see "[Adding a Node to the Cluster with Certificate Management](#)" on page 34.

To add nodes to the cluster:

1. For each node that you want to add, complete the steps in the following sections:
 - ["Keep These TCP Ports Open" on page 14](#)
 - ["Configuring the Custom Firewall Zone" on page 15](#)
 - ["Planning for a Distributed Correlation Cluster" on page 16](#)
 - ["Creating the /var/opt/arcSight Directory" on page 21](#)
 - ["Starting the Installer" on page 21](#)
 - ["Running the Installation File" on page 21](#)

2. Retrieve the installation type (fips or non fips) from the persistor node as user arcsight, run initialize-new-node-properties, and provide the requested information:

```
/opt/arcSight/manager/bin/arcSight initialize-new-node-properties
```

3. Run the createrepokey script:

```
/opt/arcSight/manager/bin/arcSight createrepokey
```

4. Start the configuration wizard:

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

5. Select the language for interface displays.
6. Specify **1** to install ESM in distributed mode.
7. Specify **1** to add to a cluster.
8. 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.

9. 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.
10. 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 [ESM Administrator's Guide](#).

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

```
sudo /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.

- a. Run `<ARCSIGHT_HOME>/bin/arcsight repositsetup`.
- 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
```

Configuring Certificate Management

Certificate Management is an optional feature that provides tools for managing both self-signed and CA signed certificates. With Certificate Management configured, all component certificates are signed by a root certificate. That root certificate is placed in the truststore of any component which requires a secure connection. Once the root certificate is in place in the truststore, any certificate signed by that root certificate will be trusted. This also means that any component will trust a new component certificate when that component's certificate is renewed. So, Certificate Management saves time because you do not have to update each certificate manually.

1. Shutdown ESM by issuing the following on the persistor node:

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

2. Enable certificate management by issuing following on the persistor node:



Note: Prior to enabling keyadmin, if you have not changed the passwords for managerkeys and clientkeys, there might be a pop up requesting you change your ESM password.

```
/opt/arcsight/manager/bin/arcsight keyadmin setup
```

3. Change the password of the managerkeys by issuing following on the persistor node:

```
/opt/arcsight/manager/bin/arcsight keyadmin changePassword --store managerkeys
```

4. Change the password of the clientkeys by issuing following on the persistor node:

```
/opt/arcsight/manager/bin/arcsight keyadmin changePassword --store clientkeys
```

5. Repeat steps 2-4 on all nodes in the cluster.

6. On the persistor, initialize certificate management by issuing:

```
/opt/arcsight/manager/bin/arcsight keyadmin initializeManagement
```

7. Choose **Distributed**.

8. Choose self-signed or CA signed.

9. Enter the list of nodes (except the persistor node) separated by commas.

10. *(Conditional)* If self-signed is chosen, the process will run to completion.

11. *(Conditional)* If CA signed is chosen, the process will create a certificate request and place it in the /opt/arcsight/manager/security/tmp directory.

12. *(Conditional)* Sign the CA certificate request, place the signed certificate in the file specified, and place the CA certificate in the file specified. All files should be in the /opt/arcsight/manager/security/tmp directory.

13. Press Enter and node will be processed.

14. Steps 11-13 will repeat for each node.

15. Restart ESM by issuing on the persistor node:

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

Adding a Node to the Cluster with Certificate Management

1. For each node that you want to add, complete the steps in the following sections:
 - ["Keep These TCP Ports Open" on page 14](#)
 - ["Configuring the Custom Firewall Zone" on page 15](#)
 - ["Planning for a Distributed Correlation Cluster" on page 16](#)
 - ["Creating the /var/opt/arcsight Directory" on page 21](#)
 - ["Starting the Installer" on page 21](#)
 - ["Running the Installation File" on page 21](#)
2. Retrieve the installation type (fips or non fips) from the persistor node as user arcsight, run initialize-new-node-properties, and provide the requested information:

```
/opt/arcsight/manager/bin/arcsight initialize-new-node-properties
```

3. Run the createrepokey script:

```
/opt/arcsight/manager/bin/arcsight createrepokey
```

4. Create the client properties file:

```
touch /opt/arcsight/manager/config/client.properties
```

5. Enable keyadmin by issuing:

```
/opt/arcsight/manager/bin/arcsight keyadmin setup
```

6. *(Conditional)* If you have ESM configured for FIPS, issue the following:

```
echo "servletcontainer.jetty311.keystore.type=BCFKS"  
>>/opt/arcsight/manager/config/server.properties
```

```
echo "servletcontainer.jetty311.truststore.type=BCFKS"  
>>/opt/arcsight/manager/config/server.properties
```

```
echo "servletcontainer.jetty311.keystore.file=config/jetty/keystore.bcfks"  
>>/opt/arcsight/manager/config/server.properties
```

```
echo  
"servletcontainer.jetty311.truststore.file=config/jetty/keystore.bcfks"  
>>/opt/arcsight/manager/config/server.properties
```

```
echo "ssl.keystore.type=BCFKS"  
>>/opt/arcsight/manager/config/client.properties
```

```
echo "ssl.truststore.type=BCFKS"
>>/opt/arcsight/manager/config/client.properties
```

```
echo "ssl.keystore.path=config/keystore.client.bcfks"
>>/opt/arcsight/manager/config/client.properties
```

```
echo "ssl.truststore.path=config/keystore.client.bcfks"
>>/opt/arcsight/manager/config/client.properties
```

- Depending on the persistor's FIPS mode, add the following line to client.properties:

Fips 192:

```
ssl.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```


Fips 128

```
ssl.cipher.suites= TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_
ECDSA_WITH_AES_256_GCM_SHA384
```

Fips 140

```
ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_
WITH_AES_128_GCM_SHA256
```


- Set the following password properties:

 **Note:** Set the password to: password.

```
/opt/arcsight/manager/bin/arcsight changepassword -f config/esm.properties
-p server.privatekey.password
```

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

- (Conditional) If you have ESM configured for FIPS, set the following password properties:

 **Note:** Set the password to: password.

```
/opt/arcsight/manager/bin/arcsight changepassword -f config/esm.properties
-p servletcontainer.jetty311.truststore.password
```

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

- (Conditional) If you have ESM configured for FIPS, reset the client keystore password:

```
/opt/arcsight/manager/bin/arcsight keyadmin changePassword --store
clientkeys
```



Note: The default password is: changeit. Set your new password to: password.

11. Create the node certificates by issuing the following on persistor:

```
/opt/arcsight/manager/bin/arcsight keyadmin renewNodeCertificates --server <node>
```

12. Start the configuration wizard:

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

13. Select the language for interface displays.
14. Specify **1** to install ESM in distributed mode.
15. Specify **1** to add to a cluster.
16. 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.

17. 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.
18. 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 [ESM Administrator's Guide](#).

19. Re-create the node certificates by issuing the following on persistor:

```
/opt/arcsight/manager/bin/arcsight keyadmin renewNodeCertificates --server <node>
```

20. To set up the services, log in as user otadmin and run the following script:

```
sudo /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.

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.

Appliance Licenses

While your appliance ships with its software already installed, you will require the ESM software license key (purchased separately).

Once the license has been installed, it will behave as a normal permanent license for ESM.

Obtaining Your License

Redeem your license on the [Software Entitlements Portal](#), then download the license file to a computer from which you can connect to your appliance.

For more information, refer to the software delivery confirmation email you received from OpenText.

Chapter 3: Converting from Compact to Distributed Mode

If you previously set up the ESM E8400 appliance in compact mode, you can convert the system to distributed correlation mode.

Prior to performing the conversion, you must complete the following steps on the persistor node (E8400 appliance):

- Open the correct ports. For more information, see ["Keep These TCP Ports Open" on page 14](#).
- Configure the custom firewall zone. For more information, see ["Configuring the Custom Firewall Zone" on page 15](#).
- Plan the cluster. For information about cluster planning, see ["Planning for a Distributed Correlation Cluster" on page 16](#).
- Ensure that information repository instances will not run on the disk partition that contains `/opt/arcsight`. 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 upgrade ESM. If `/var/opt/arcsight` does not meet the requirements that are listed below, the upgrade program will generate an error and will not continue. During the upgrade, the upgrade program moves repository data to the partition that contains `/var/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.

To create the `/var/opt/arcsight` directory, see ["Creating the `/var/opt/arcsight` Directory" on page 21](#).



Note: To convert from compact mode to distributed correlation mode, each server host name must resolve to an IP address for each cluster node. Otherwise, the conversion process will fail with an error message.

To convert your system from compact mode to distributed correlation mode:

1. Verify that all services are running:

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

2. Change to the arcsight user.

3. Stop the ArcSight Manager:

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

4. Change directory to /opt/arcsight/manager.

5. Initialize distributed correlation mode:

```
bin/arcsight initialize-distributed-mode
```

6. Set up the information repository, using the option **Change the TCP Port Range for ESM Processes** to specify the port range:

```
bin/arcsight reposetup
```

For more information about reposetup, see the [ESM Administrator's Guide](#).

7. Run managersetup:

```
bin/arcsight managersetup
```

For more information about managersetup, see the [ESM Administrator's Guide](#).



Important: Do not start the ArcSight Manager after managersetup is complete.

8. Initialize certificate administration and create a password for certificate administration:

```
bin/arcsight certadmin -init
```



Note: Keep track of the password you specify. It will be required during the next section ("To complete configuration and bring up the services") and whenever you add new nodes the cluster in the future.

For information about password restrictions, see the [ESM Administrator's Guide](#).

9. Add the version information for this node:

```
/etc/init.d/arcsight_services setLocalBuildVersions
```

10. If you need a distributed cache instance on the persistor node, run the following command:

```
bin/arcsight dcachesetup
```

For more information about `dcachesetup`, see the [ESM Administrator's Guide](#).

11. To install ESM on the remaining cluster nodes, see the "Adding Nodes to a Cluster" section of "Installing Software ESM in Distributed Correlation Mode Using the Configuration Wizard" on page 22.

After you have added all the nodes, proceed to the next section.

To complete configuration and bring up the services:



Note: Run these commands on the persistor node, as user `arcsight`, from the `/opt/arcsight/manager` directory.

1. Set up passwordless SSH:

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

2. Change directory to `/opt/arcsight/manager`.

3. Review and approve all certificates:

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

Review the output to verify that the certificates represent the nodes where the ArcSight Manager or correlation services were installed. To view the certificate details, use the `-v` option.

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

```
bin/arcsight certadmin -approveall
```

5. Stop all services:

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

6. Start the repository service:

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

7. Set up message bus control and message bus data:

```
bin/arcsight mbussetup
```

For more information about `mbussetup`, see the [ESM Administrator's Guide](#).

8. If you need additional repository instances, run the following command:

```
bin/arcsight reposetup
```

For more information about `reposetup`, see the [ESM Administrator's Guide](#).

9. *(Conditional)*: If compact system had certificate management enabled, perform the following:

- a. On the persistor shutdown the repository instances

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

- b. On each new node run the following from the `/opt/arcsight/manager` directory:

```
bin/arcsight keyadmin setup
```

```
bin/arcsight keyadmin changePassword --store clientkeys (set a password at least 6 characters in length)
```

```
bin/arcsight keyadmin changePassword --store managerkeys (set a password at least 6 characters in length)
```

- c. On the persistor from the `/opt/arcsight/manager` directory re-enable Certificate Management:

```
bin/arcsight keyadmin initializeManagement
```

10. Start all services, which will bring up services related to distributed correlation mode:

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

11. Verify that all services are running:

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

Chapter 4: Restore Procedures


OpenText recommends to perform backups of the information and configuration of an ESM appliance to ensure you can recover your data in case of loss.

Components should be backed up on a regular schedule, as well as before you upgrade your environment.

Restoring an Appliance to Factory Settings

You can restore appliances to their original factory settings by using the procedures detailed here. To perform a restore procedure, you will require:

- An `.iso` image file containing the factory settings for the version of ESM you are restoring. Find the name of the file in the **Downloading Your Factory Restore Image Files** section of the [EC8300 Appliance Release Notes](#).

 Once you have acquired the image file, please refer to the [signature verification](#) instructions, and perform the verification steps before starting the procedure below.

The restore procedure can be conducted in two ways:

- If you have physical access to the appliance, use the ["Restoring an Appliance Using a USB Memory Stick" below](#) method
- If you have only iDRAC access to the appliance, use the ["Restoring an Appliance Using iDRAC Access" on page 44](#) method

Restoring an Appliance Using a USB Memory Stick

This method will require the following external hardware:

- A 32 GB or higher USB memory stick (the faster type available, but at least USB 2.0 or 3.x)
- A Linux machine to perform the burning of the `.iso` image into the USB memory stick

Image Burning

1. Connect the USB memory stick to one of the ports of the Linux machine.
2. From the command line, execute the following command to burn the `.iso` image into the USB memory stick:

```
dd if=<iso_image_file_name>.iso status=progress oflag=sync of=/dev/sdX  
bs=1M
```

Where

- <iso_image_file_name> is the name of the image file downloaded [here](#).
- /dev/sdX is the device name of your USB drive (e.g.,/dev/sdb).

And wait until the progress has reached 100%.

3. Turn your appliance off and connect the bootable USB stick you just created to one of its ports. Reboot the appliance.

Restore Procedure:

1. Access the remote console of the appliance through iDRAC.

If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

["Setting Up the Appliance for Remote Access" on page 9](#)

2. From the iDRAC **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.

4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

A pop-up window will request to **Confirm Power Action**. Select **Yes**.

5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select your USB stick (its name will depend on brand and model, but it will start with **Disk connected to back USB**).
7. The appliance will boot from the selected USB stick.

The restore process will start automatically if you allow it some time, or you can click on the **ArcSight** option at the top to start right away.

8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 20 minutes. Once the restore process has reached this point:

```
The next step: true
Now run: true
```

Your input will be required to reboot the appliance:

reboot

9. Once the reboot process is finished, follow the instructions listed in:
 - "[Initializing the ESM Appliance](#) " on page 10

Restoring an Appliance Using iDRAC Access



When using the iDRAC Remote File Share feature to perform the restore procedure, make sure there is no USB drive connected to the appliance ports, since its presence may interfere with the restore process.

This method will require the following preparation:

- Store your .iso image in a location that is accessible to the iDRAC network. For more information, see the [iDRAC documentation](#).
- Configure the iDRAC Remote File Share option in the Virtual Media tab using shared the .iso image downloaded [here](#).

Restore Procedure:

1. Access the remote console of the appliance through iDRAC.

If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

"[Setting Up the Appliance for Remote Access](#)" on page 9
2. From the iDRAC **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.
4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

A pop-up window will request to **Confirm Power Action**. Select **Yes**.
5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select **Virtual Network File**.
7. The appliance will boot from the .iso image in the Remote File Share.

The restore process will start automatically if you allow it some time, or you can click on the **ArcSight** option at the top to start right away.

8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 20 minutes. Once the restore process has reached this point:

```
The next step: true  
Now run: true
```

Your input will be required to reboot the appliance:

```
reboot
```

9. Once the reboot process is finished, follow the instructions listed in:
["Initializing the ESM Appliance " on page 10](#)

Publication Status

Released: Wednesday, December 4, 2024

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 Administrator's Guide to Hardware Appliances for ArcSight ESM (8300 Appliance 24.4)

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!