

# **Configuration Guide**

---

ESM Appliance

ArcSight ESM 6.0c  
with CORR-Engine

March 1, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

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

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

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

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

This document is confidential.

## Contact Information

---

<b>Phone</b>	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
<b>Support Web Site</b>	<a href="http://support.openview.hp.com">http://support.openview.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

---

## Revision History

---

Date	Product Version	Description
03/01/2013	ArcSight ESM 6.0c with CORR-Engine	First release of the Configuration Guide for the ESM Appliance model E7400, with ESM 6.0c with CORR-Engine

---

# Contents

---

- Chapter 1: Configuring the ESM Appliance ..... 5**
  - Installation Files and Documentation ..... 5
  - Configuring the Operating System ..... 5
    - Configuring Network Settings ..... 6
    - Synchronizing Time over the Network ..... 6
  - Creating a Password for the **arcsight** User ..... 7
  - Installation ..... 7
    - Installing ArcSight ESM 6.0c ..... 7
    - Installing ArcSight Console ..... 7
    - Installing ArcSight Forwarding Connector ..... 7
  - Related Documentation ..... 8
- Chapter 2: Restoring Factory Settings ..... 9**



# Chapter 1

## Configuring the ESM Appliance

---

This document includes the following topics to help you configure the ESM Appliance:

- ["Installation Files and Documentation" on page 5](#)
- ["Configuring the Operating System" on page 5](#)
- ["Creating a Password for the arcsight User" on page 7](#)
- ["Installation" on page 7](#)
- ["Related Documentation" on page 8](#)

## Installation Files and Documentation

The following files are available in the `/opt/arcsight/installers` directory:

- The ESM Suite installer, `ArcSightESMSuite.bin`, which includes installations for the Manager, CORR-Engine, and ArcSight Web
- Installation and Configuration Guide for ArcSight ESM 6.0c with CORR-Engine
- Release Notes for ArcSight ESM 6.0c with CORR-Engine

## Configuring the Operating System

The ESM Appliance has the Red Hat Enterprise Linux (RHEL) operating system installed. Set up the preferences for RHEL when you boot the system for the first time or when you boot the system after a factory restore.

The Setup Agent wizard will help you set the preferences for Red Hat Enterprise Linux. The first time the system is started, the wizard displays the Welcome panel.

- 1 On the Welcome panel, click **Forward**.
- 2 On the License Information panel, read the terms of the license agreement. Choose **Yes, I agree to the License Agreement** and click **Forward**.
- 3 On the Keyboard panel, select the appropriate keyboard for your locale and click **Forward**.
- 4 On the Root Password panel, enter a password for the root account which is used for system administration. Re-enter to confirm it, then click **Forward**.
- 5 On the Date and Time panel, keep the default date and time on the calendar and time fields for now and ignore the option to synchronize the date and time over the network. You will do this in a separate procedure. Click **Forward**.

- 6 Skip the fields in the Create User panel and click **Finish**.



The ESM Appliance has the user defined as `arcsight`. You will set a password for it in a separate procedure.

The login screen is displayed.

- 7 Click **Other**, then log in as **root** with the root password you entered in [Step 4](#).

Proceed to [Configuring Network Settings](#).

## Configuring Network Settings

You need to enter network settings manually on the appliance. Perform the following steps after you have attached a network connection to a physical port.

- 1 As root, choose **System > Preferences > Network Connections**.

The Network Connections dialog displays the Wired tab.

- 2 Choose the port number corresponding to the network-connected physical port and click **Edit**.

On the Wired tab, `eth0` corresponds to the first physical port, `eth1` to the second physical port, and so on.

- 3 Enter the appliance's IP address by changing the displayed default entry.
- 4 Add the DNS servers as applicable to your environment and optionally search domains for the ESM Appliance.
- 5 Click **Apply**.
- 6 Restart the network port using the following command as an example:

```
/etc/init.d/network restart
```

Proceed to [Synchronizing Time over the Network](#).

## Synchronizing Time over the Network

Using NTP servers is strongly recommended, since accurate time keeping is essential for event correlation and log management.

- 1 As root, choose **System > Administration > Date & Time**.
- 2 Click **Synchronize date and time over the network**.
- 3 In the NTP servers text box, specify one or more NTP servers with which the appliance synchronizes to obtain time. You have the option to retain the default NTP servers and add your own to the list, or replace the entries with your own.

Every time you add a server, the appliance attempts to contact it. If the connection succeeds, the server is added to the list. If the server you just added is unreachable at this time, you still have the option to add it.

- 4 Click **OK**.

Proceed to [Creating a Password for the `arcsight` User](#).

## Creating a Password for the `arcsight` User

The user called `arcsight` has been defined in the appliance. Create a password as follows:

- 1 Log in as **root**.
- 2 Create a password with the following command:  
**passwd arcsight**
- 3 Enter a new password when prompted. Re-enter it to confirm.

## Installation

The following setups have been preconfigured in the appliance:

- Open ports
- Space for the partition with `/tmp` directory
- User process limit (`ulimit`)
- Creation of `/opt` with XFS format
- Creation and setting permissions for `/opt/arcsight`

Refer to the Installation and Configuration Guide for ESM 6.0c with CORR-Engine for installation procedures. While reading the guide, skip the procedures for the above setups.

## Installing ArcSight ESM 6.0c

- 1 Log in as **arcsight** and use the password you configured in [Creating a Password for the `arcsight` User](#).
- 2 Go to the `/opt/arcsight/installers` directory.
  - a Proceed to page 17 of the Installation and Configuration Guide.
  - b Skip the procedures to untar `ArcSightESMSuite` because this file is provided in the `bin` format with the proper execute permission.
  - c Follow the instructions under the heading, *Running the Installation File*.

## Installing ArcSight Console

Install ArcSight Console on a separate system, not on the appliance.

For instructions, refer to the Installation and Configuration Guide for ESM 6.0c with CORR-Engine, chapter on Installing ArcSight Console. The chapter contains information on supported platforms for your guidance. Then, download the software corresponding to your preferred platform from [HP Software Support Online](#). The ArcSight Console has its own user's guide. See ["Related Documentation" on page 8](#) for information on how to get the guide.

## Installing ArcSight Forwarding Connector

Download and manually install ArcSight Forwarding Connector version 5.2.5.6403.0 from [HP Software Support Online](#). Download the Forwarding Connector User's Guide and Release Notes from [Protect 724](#).

## Related Documentation

The complete documentation set for ESM 6.0c with CORR-Engine is available from [Protect 724](#). On the documentation page, click **ArcSight ESM** and **ArcSight Express Documentation**, then click **ESM 6.0c with CORR-Engine**.



## Chapter 2

# Restoring Factory Settings

---

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



System Restore permanently deletes all event and configuration data and restores the appliance to its original factory settings. If necessary, work with your HP Customer Support representative for ArcSight products before proceeding.

### To restore the ESM Appliance to its original factory settings:

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

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



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

- 4 Use the mouse or arrow keys to select **System Restore (xxxxx)** and press **Enter**.  
System Restore automatically detects and displays the archive image. The image is named following this pattern:  
  
`YYYY-MM-DD_E7400_XXXXX.ari`  
  
where YYYY-MM-DD is the date, E7400 is the appliance model, and XXXXX corresponds to the release's build number.
- 5 Optionally press **F10** (VERIFY) to check the archive for damage before performing the restore. If necessary, contact HP Customer Support for ArcSight products for assistance.
- 6 Press **F1** (AUTOSELECT) to automatically map the source image.
- 7 Press **F2** (RESTORE) to begin the restore process.
- 8 Press **y** to continue.

Progress bars show the status of the restoration.



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

- 9 When the restore process is completed, press **F12** to reboot the appliance, then press **y** to continue.
- 10 You can now configure the appliance again. Refer to [“Configuring the ESM Appliance” on page 5](#) for details.



When following the instructions to install ArcSight ESM, make sure you are installing the correct build. Contact HP Customer Support for ArcSight products if you have questions.