

Configuration Guide

ArcSight™ ESM Appliance v5.0 SP1

March 5, 2011



Configuration Guide, ArcSight™ ESM Appliance v5.0 SP1

Copyright © 2011 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
3/5/11	ESM v5.0 SP1	Released with ESM v5.0 SP1

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal
Customer Forum	https://protect724.arcsight.com

Contents

Chapter 1: Configuring ArcSight™ ESM Appliance 5

 Configuring the Operating System 5

 Installing ArcSight™ ESM Components 8

 Preparing to Install the Oracle Database 9

 Oracle Installation 9

Chapter 2: Restoring Factory Settings 11

Configuring ArcSight™ ESM Appliance

This document covers the following topics:

- "Configuring the Operating System" on page 5
- "Installing ArcSight™ ESM Components" on page 8
- "Preparing to Install the Oracle Database" on page 9

Configuring the Operating System

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 only or when you boot the system after a factory restore.

The 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 Agreement** panel, read the terms of the license agreement. Select **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 and click **Forward**.

The next step is to configure the IP addresses for the appliance on the Network Setup panel. The appliance is set up with the following pre-defined IP addresses:

- ◆ 192.168.35.35 for eth0
- ◆ 192.168.36.35 for eth1
- ◆ 192.168.37.35 for eth2
- ◆ 192.168.38.35 for eth3



Note

eth0 corresponds to the first physical port, eth1 to the second physical port, and so on.

If you plan to configure a single network interface, make sure to configure the **eth0** interface. Configuring eth1 as the single network interface will cause the Manager to not communicate with the database.

- 5** On the Network Setup panel, click **Change Network Configuration**.

The Network Configuration panel appears.



For the Network Setup panels, note that if you click on the wizard panel when the Network Setup panel is in the foreground, the panel disappears and the wizard buttons remain inoperable. Use **Alt-Tab** to switch back to the Network Setup panel.

- 6 On the **Network Configuration** panel's **Devices** tab, select **eth0** and click **Edit**.
 - a On the **Ethernet Device** panel's **General** tab, verify that **eth0** is displayed as Nickname. Select **Activate device when computer starts**.
 - b Set the IP address, subnet mask, and default gateway.



Make sure that the IP address you set up is available. The First Boot Wizard will report errors if the IP address has not been configured correctly.

- c Click **OK**.
- d For ports that will not be used, repeat from [Step 6](#) to select the port (for example, eth1) and edit it. This time, uncheck the option to activate the device when the computer starts and skip setting the static IP addresses. Click **OK** when you have completed editing each remaining port.

The wizard displays the Network Configuration panel. Entering information here requires familiarity with your network environment, such as IP addresses of critical servers, to ensure communication between the appliance and those servers.

- 7 On the **Network Configuration** panel's **DNS** tab:

- a** Enter the hostname for the appliance in the **Hostname** field. The hostname must be recognized by your domain name server (DNS).

The default hostname for the appliance is **esm**. Make sure your hostname can be resolved by your name server. If you prefer to use your own hostname for the appliance, add that hostname in the DNS tab; then add it again in the Hosts tab and set the other required values. Ensure that you can ping this host.

- b** Enter the IP address of your DNS in the **Primary DNS** field.
- c** Click **OK**.
- d** Select **File->Save** to save your changes.
- e** Select **File->Quit** to exit the Network Configuration panel.

- 8** On the **Network Setup** panel, click **Forward**.

- 9** On the **Firewall** panel:

- a** Select **Enabled** in the Firewall dropdown menu.
- b** Select **SSH**. The other trusted services on the list are not required.

Make sure the ports listed in the note below are open.



Note

Make sure that the ports 8443 and 9443 are open for outgoing communications. The ArcSight Manager uses port 8443 and the ArcSight Web uses port 9443 for communication. Leave port 22 open for remote [ssh](#) access.

- c** Click **Forward**.

- 10** On the **SELinux** panel, click **Forward**.

- 11** On the **Date and Time** panel, select the **Network Time Protocol** tab if not already displayed.

Network Time Protocol (NTP) is enabled by default. Keep this setting. This will configure the operating system to use the NTP servers specified in the list from which to obtain the time.

- a** Click **Add**.
- b** In the **New NTP Server** field, enter the NTP server you are using. Make sure there are no firewalls blocking connections from the appliance to this NTP server.
- c** Click **Forward**. Wait for the NTP server to be contacted.

It may take a few minutes to contact the server. If the system cannot contact the server, the request will time out in a few minutes and will take you to the next panel in the wizard. Make sure to resolve connectivity issues after completing the setup process.

The list of servers configured by default points ESM Appliance to a virtual cluster of time servers operated by the NTP project. Assuming that UDP port 123 is open to the

outside internet in your firewall, you can keep the default values, unless you would prefer to use your own cluster of NTP servers.



Using NTP is strongly recommended, since accurate time keeping is essential for event correlation and log management. But if you choose to de-activate the Network Time Protocol, set the local date and time in the Date & Time tab.

The wizard displays the Create User panel. You will use this panel to enter a user for ArcSight ESM.

- 12** On the **Timezone** panel, select the Timezone in which your ESM Appliance is located and click **Forward**.

- 13** On the **Create User** panel, create a user for the ArcSight system.

- ◆ **Username**—The user name, for example, **arcsight**.
- ◆ **Full Name**—A descriptive name for the user name (optional).
- ◆ **Password**—The password for the user.
- ◆ **Confirm Password**—The password for the user, entered a second time to confirm.

Click **Forward**.

- 14** On the **Sound Card** panel, click **Forward**.

- 15** On the **Additional CDs** panel, click **Finish**.

The login screen is displayed.

- 16** Log in with the root password you entered in [Step 4 on page 5](#).

- 17** Reboot the appliance.



It is important that you reboot the appliance after completing the OS setup. Rebooting the appliance ensures that your network settings are saved.

You are now ready to proceed with the installation of the ArcSight ESM software components.

Installing ArcSight™ ESM Components

The installation files for ArcSight ESM components are available in the [/opt/arcsight/installers](#) directory. Navigate to this directory and install the following ESM components according to the instructions found in the *ArcSight ESM Installation and Configuration Guide*.

- 1** ArcSight Database (see instructions below in ["Preparing to Install the Oracle Database" on page 9](#) and ["Oracle Installation" on page 9](#))
- 2** ArcSight Manager
- 3** ArcSight Web
- 4** Download the Console installer file on one or more systems from the ArcSight Customer Support website and install the Console on those systems.

Preparing to Install the Oracle Database

Before you install the ArcSight Database, note the following recommendations:

- There are six physical disks set up in a RAID 10 group that shows up as a single logical disk to the Operating System. This is partitioned such that there is approximately 1.6 TB on `/opt/data` and 97 GB on the root directory, `/`. ArcSight recommends that you:
 - ◆ Install the ArcSight Database in the `/usr/local/arc sight/db` directory
 - ◆ Set the Oracle user home and installation directory as `/home/oracle` and Oracle Home as `/home/oracle/OraHome11g`.
 - ◆ Store Redo Logs and default Oracle data files (System, SysAux, and so on) under the default `/home/oracle/OraHome11g/oradata/arc sight`.
 - ◆ Store data files for all ArcSight tablespaces (ARC_*) in `/opt/data`.
 - Estimate your retention needs and whether you want to enable partition archiving or not. Contact ArcSight Support if you need help on this. As a guideline, you can completely fill the `/opt/data` directory with data files. However, if you enable partition archiving and also use `/opt/data` for storing archived partitions, you need to do proper sizing estimates based on how many days worth of data you want to retain in the online and offline partitions so that the disks don't fill up completely.
- Refer to the *ArcSight ESM Installation and Configuration Guide*, chapter on *Installing ArcSight Database*, for additional information.
- Review the section, *Preparing a Linux System*, steps 5-7 in the *ArcSight ESM Installation and Configuration Guide* for details about how to configure and verify that the hostname is set and it can be pinged. The Oracle installation will fail if your host system cannot be pinged.

Oracle Installation

For a successful Oracle setup, follow the tips provided in this section during Oracle installation.



Note

Where to find complete instructions

- For complete instructions about how to install the Oracle database, see the *ArcSight ESM Installation and Configuration Guide*.
- To verify that Oracle initialization was successful, and for instructions about how to administer and maintain ArcSight ESM, see the *ArcSight ESM Administrator's Guide*.
- Review the Release Notes for the ESM version installed on your appliance, available on the ArcSight Customer Support site, <http://www.arcsight.com/supportportal>.

- When you get to the prompt to set the ArcSight Database Template, ArcSight recommends using the Extra Extra Large template. The Extra Extra Large Template dedicates 12 GB out of 36 GB physical memory for Oracle, leaving enough memory for the Manager, operating system, and any other ArcSight components you need.
- After the Oracle installation is completed, apply the Oracle critical patch update (CPU) included with your ArcSight ESM Appliance. The CPU and the OPatch utility used to install it are available in the `installers/oracle` folder.
- After the CPU is applied, install the ArcSight Manager in the `/home/arc sight/` directory, for example, `home/arc sight/manager<version#>`.

You may begin using the appliance after rebooting. To access ESM using the Console, install the ESM Console according to the instructions in the *ArcSight ESM Installation Guide*. You must install the Console in another system.

Restoring Factory Settings

ArcSight ESM Appliance can be restored to its original factory settings using the built-in Acronis True Image software.

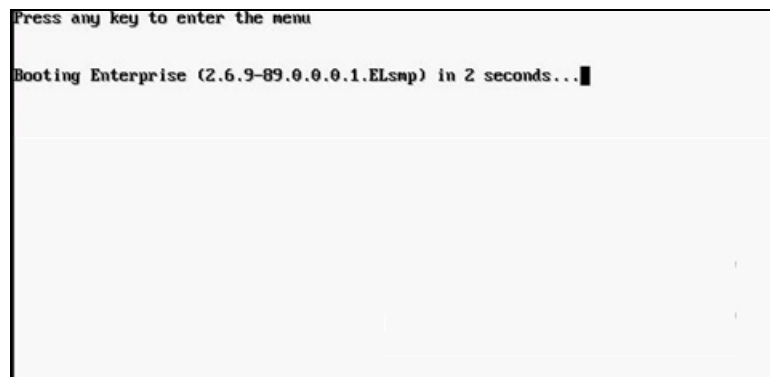


Factory reset deletes all event and configuration data

Restoring ArcSight ESM Appliance to factory settings will permanently delete all event data and configuration settings.

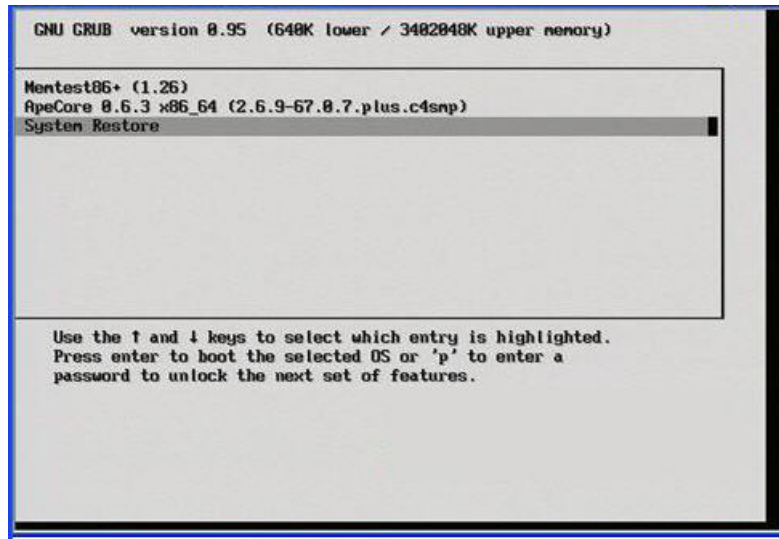
To restore the ArcSight ESM Appliance to its original factory settings, perform these steps:

- 1 Attach a keyboard, monitor, and mouse directly to the ArcSight ESM Appliance system.
- 2 Reboot the ArcSight ESM Appliance from the GUI. Click **Setup > System Admin > Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
- 3 When the following screen appears, press any key.



This screen 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 A screen similar to the following appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press Enter.



- 5 Click **Acronis True Image Server** to continue.
- 6 In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press Enter.
- 7 When the Restore Data Wizard starts, click **Next** to continue.
- 8 On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.
- 9 On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.
- 10 On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** and click **Next**.
- 11 On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.
- 12 On the **NT Signature selection for image restoration** page, select **Generate new NT signature** and click **Next**.
- 13 On the **Restored Hard disk Location** page, select the **cciss/c0d0** drive to restore and click **Next**.
- 14 On the **Non-empty Destination Hard Disk Drive** page, select **Yes, I want to delete all the partitions on the destination hard drive before restoring** and click **Next**.
- 15 On the **Next Selection** page, select **No, I do not** and click **Next** (there are no other partitions or disks to restore).
- 16 Validating the archive before restoring is optional. On the **Restoration Options** page:
 - a Select **Validate backup archive for the data restoration process** if you want to validate before resetting the appliance,

Or

Select **Reboot the computer automatically after the restoration is finished** if you want to reboot the appliance automatically.

b Click **Next**.

- 17** Review the checklist of operations to be performed and click **Proceed** to begin the restore process, or click **Back** to revisit previous pages and make changes as required.



Do no interrupt restore process

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

Progress bars show the status of the current operation and the total progress.

- 18** When you see a message indicating that the data was restored successfully, click **OK**.
- 19** If you specified automatic reboot in [Step 16](#), the appliance reboots when the restore is complete. Otherwise, reboot the appliance manually.

