

Configuration Guide

ArcSight™ Express v5.0 SP1 Patch 1

March 10, 2011



Configuration Guide ArcSight™ Express v5.0 SP1 Patch 1

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
3/10/11	ArcSight™ Express v5.0 SP1 Patch 1	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/
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: What is ArcSight Express?	5
Pre-installed Components on ArcSight Express Appliance	5
ArcSight Manager	6
ArcSight Database	6
ArcSight Web	6
ArcSight Forwarding Connector	6
Pre-installed Components on ArcSight Storage Appliance	6
ArcSight Logger	6
ArcSight Connector Management	7
ArcSight Console	7
Deployment Overview	7
ArcSight Express Communication Overview	8
Effect on Communication when Components Fail	8
Related Documents	9
Chapter 2: Configuring ArcSight Storage Appliance	11
Define Storage Volume	12
Create Storage Groups	12
Configure NTP	12
Configure Indexing	13
Reboot the Appliance	13
Create SmartMessage Receivers	13
Adding an ArcSight Storage Appliance	13
Chapter 3: Configuring ArcSight Express Appliance	15
Configuring ArcSight Express Appliance	15
Configuring the Operating System	15
Configuring Software Components on ArcSight Express Appliance	20
The Next Steps	23
Chapter 4: Installing ArcSight Console	25
Console Supported Platforms	25
Installing the Console	26
Transferring Configuration from an Existing Installation	27

Selecting the Mode in which to Configure ArcSight Console	28
Manager Connection	28
Authentication	30
Web Browser	31
User Logs and Preferences	31
Starting the ArcSight Console	32
Logging into the Console	32
Creating ArcSight Express Users	33
Reconnecting to the ArcSight Manager	33
Reconfiguring the ArcSight Console	34
Uninstalling the ArcSight Console	34
Chapter 5: Using SmartConnectors with ArcSight Express	35
Installing the SmartConnector	35
Importing the Manager's Certificate	36
Using keytoolgui to Import the Manager's Certificate	36
Exporting the Manager's Certificate	36
Importing the Manager's Certificate into the SmartConnector's Truststore	37
Import the Manager's certificate using the Connector Manager	38
Appendix A: Troubleshooting	39
Location of Log files for Components	39
Customizing ESM Components Further	40
Fatal Error when Running the First Boot Wizard	41
Manager Service Failed when Starting	42
"Failed" Status while Configuring or Starting a Component	42
Changing the IP Address of the ArcSight Express Appliance After Configuring It in the First Boot Wizard	44
Changing the Host Name of the ArcSight Express Appliance After Configuring It in the First Boot Wizard	46
Appendix B: Default Settings for Components	49
General	49
ArcSight Database	49
About Data Retention on ArcSight Express	51
ArcSight Manager	51
About ArcSight Web	52
ArcSight Forwarding Connector	52
ArcSight Logger	53
Appendix C: Restoring Factory Settings	55
Index	57

What is ArcSight Express?

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for security monitoring by leveraging ArcSight ESM's superior correlation capabilities in combination with a ArcSight Storage Appliance. ArcSight Express delivers an easy-to-deploy enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules and reports included as part of ArcSight Express Content.

This chapter covers the following topics:

- ["Pre-installed Components on ArcSight Express Appliance" on page 5](#)
- ["Pre-installed Components on ArcSight Storage Appliance" on page 6](#)
- ["ArcSight Console" on page 7](#)
- ["Deployment Overview" on page 7](#)
- ["ArcSight Express Communication Overview" on page 8](#)
- ["Related Documents" on page 9](#)

The ArcSight Express solution can be comprised of the following appliances:

- **ArcSight Express Appliance**
The ArcSight Express Appliance comes with ArcSight Database, ArcSight Manager, ArcSight Web and ArcSight Forwarding Connector pre-installed on it.
- **ArcSight Storage Appliance**
The ArcSight Storage Appliance serves as a long term data storage hardware solution that receives and stores events, and supports search and retrieval of the stored events. It has the ArcSight Logger software pre-installed on it. The ArcSight Storage Appliance comes as a standard component with certain models of ArcSight Express only. However, you can purchase the ArcSight Storage Appliance separately for models of ArcSight Express with which it is not included.

Pre-installed Components on ArcSight Express Appliance

The ArcSight Express Appliance has the following software components pre-installed on it:

- ArcSight Manager
- ArcSight Database
- ArcSight Web
- ArcSight Forwarding Connector

ArcSight Manager

ArcSight Manager is at the center of the ArcSight Express Appliance. The Manager is a software component that functions as a server that receives event data from Connectors and correlates and stores them in the database. The Manager also provides advanced correlation and reporting capabilities. The ArcSight Web interface is used to retrieve this information from the Manager and display it.

ArcSight Database

ArcSight Database is the central repository for all information collected by the ArcSight Manager and is based on Oracle DBMS. It also stores the configuration information for users, groups, rules, dashboards, assets, and reports.

ArcSight Web

ArcSight Web is the primary user interface for ArcSight Express. ArcSight Web is a web server component that enables you to access ArcSight Manager securely using a browser. ArcSight Web supports the following browsers on the Windows Vista or Windows XP platforms:

- Internet Explorer 7 and 8
- Safari on Macintosh 4
- Firefox on Windows and Linux 3.0 - 3.6
- Firefox on Macintosh 3.6



Check the Product Lifecycle document available on the ArcSight Customer Support website for information on the exact browser versions supported.

ArcSight Web is an easy-to-use interface designed for operators in a Security Operations Center (SOC) and customers of a Managed Security Service Provider (MSSP) who need to view information on the Manager.

ArcSight Forwarding Connector

The ArcSight Forwarding Connector is a component that transports events from the ArcSight Express Appliance to the ArcSight Storage Appliance.

Pre-installed Components on ArcSight Storage Appliance

The ArcSight Storage Appliance comes installed with the following software:

ArcSight Logger

ArcSight Logger is a log management solution that is optimized for extremely high event throughput. Logger stores time-stamped text messages, called events, at high sustained input rates and can optionally forward selected events. Logger compresses raw data, but can always retrieve unmodified data on demand, for forensics-quality litigation data.

ArcSight Connector Management

ArcSight Connector Management software incorporates a number of onboard ArcSight SmartConnectors and a web-based user interface that provides centralized management for SmartConnectors.

SmartConnectors are ArcSight software components that forward security events from a wide variety of devices and security event sources to ArcSight Logger.

You have the option to use up to four SmartConnector(s) locally depending on available resources on the ArcSight Storage Appliance.

ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks on ArcSight Express, such as fine tuning the pre-installed ArcSight Express content and managing users. ArcSight Console is not bundled with ArcSight Express and should be separately installed on a system other than the ArcSight Express Appliance.

Deployment Overview

The following is an example of how various ArcSight components are normally deployed in a network.

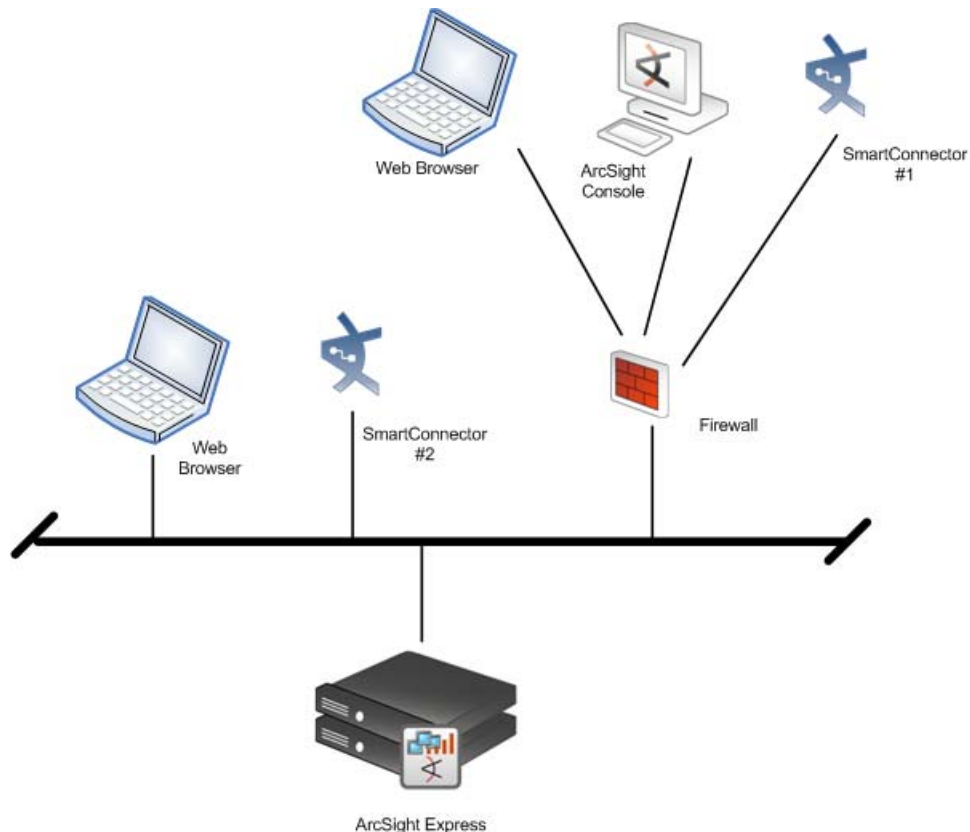


Figure 1-1 ArcSight Express Deployment Overview

ArcSight Express Communication Overview

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

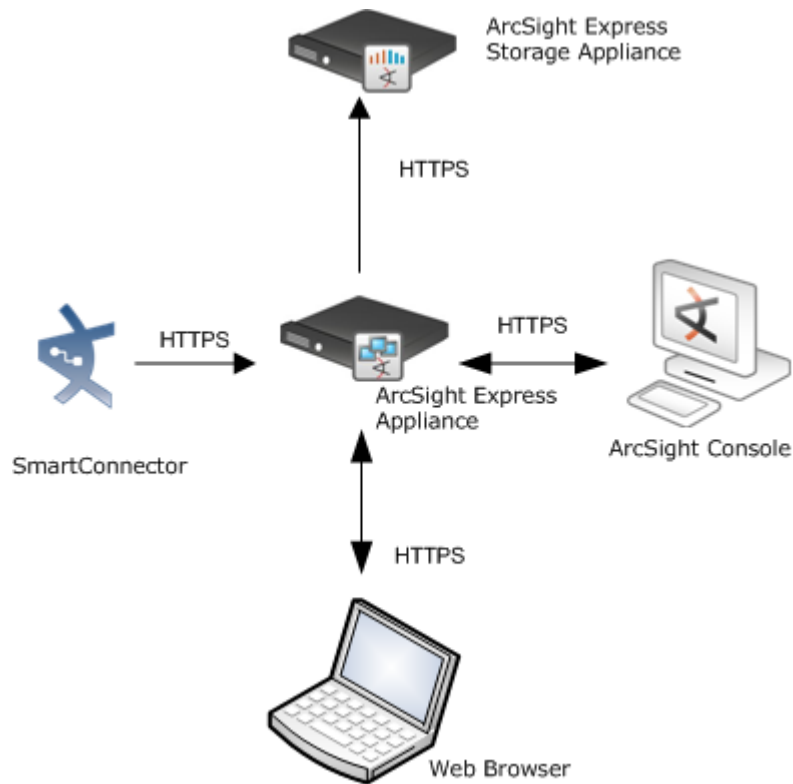


Figure 1-2 ArcSight Express Solution - Communication Overview

SSL works over TCP (Transport Control Protocol) connections. The default incoming TCP port on ArcSight Manager is 8443, for ArcSight Web it is 9443, and for ArcSight Storage Appliance it is 443.

The Manager never makes outgoing connections to the Console, ArcSight Web, or SmartConnectors. The Manager connects to the Database on the appliance locally using JDBC.

Effect on Communication when Components Fail

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

If the database is unavailable for any reason, such as when database is filled to capacity, the Manager stops accepting events and caches any events that were not committed to the database. The SmartConnectors also start caching new events they receive, so there is no event data loss. The Console gets disconnected. All existing ArcSight Web connections are disconnected and no new login requests to the Web server are accepted until the database is up and running again.

If the Manager is unavailable, the SmartConnectors start caching events to prevent event data loss. The database server is idle. The Console is disconnected. All existing ArcSight Web connections are disconnected and no new login requests to the Web server are accepted.

If a SmartConnector fails, whether event data loss will occur or not depends on the SmartConnector type. SmartConnectors that listen for events from devices such as the SNMP SmartConnectors will stop accepting events. However, a SmartConnector that polls a device, such as the NT Collector SmartConnector, may be able to collect events that were generated while the SmartConnector was down, once the SmartConnector comes back up.

If the Forwarding Connector fails, the Manager will continue to store the events in its file store which is 10 GB in size. If the file store gets filled up, the Manager will start dropping the oldest events and the newer events will continue to get stored on the file store.

If the ArcSight Storage Appliance fails, the Forwarding Connector will cache the events that were supposed to be forwarded to the ArcSight Storage Appliance.

Related Documents

To get you started, *Getting Started with ArcSight Express* document is available in hard copy and is packaged with ArcSight Express.

The ArcSight Express Online Help is available from the ArcSight Console. Also, in addition to this guide, you can refer to and download the following documents from the ArcSight Customer Support download site:

- *Getting Started with ArcSight Express*
- *Getting Started with ArcSight Logger*
- *ArcSight Logger Administrator's Guide*
- *ArcSight ESM Release Notes*
- *ArcSight ESM Installation and Configuration Guide*
- *ArcSight ESM Administrator's Guide*
- *SmartConnector Configuration Guide for ArcSight Forwarding Connector*
- *SmartConnector User's Guide*
- *ArcSight Express Release Notes*

Chapter 2

Configuring ArcSight Storage Appliance

This chapter covers the following topics:

- ["Define Storage Volume" on page 12](#)
- ["Create Storage Groups" on page 12](#)
- ["Configure NTP" on page 12](#)
- ["Configure Indexing" on page 13](#)
- ["Reboot the Appliance" on page 13](#)
- ["Create SmartMessage Receivers" on page 13](#)
- ["Adding an ArcSight Storage Appliance" on page 13](#)

After you have set up the hardware for ArcSight Express, the next step is to initialize the the ArcSight Storage Appliance if applicable. ArcSight Storage Appliance (Storage Appliance) is included with certain models of ArcSight Express.

The ArcSight Express Storage Appliance is also known as ArcSight Logger when purchased separately. Refer to the *ArcSight Logger Administrator's Guide* for details on how to configure ArcSight Storage Appliance. You can download this guide from the ArcSight Customer Support download site.

It is very important that you initialize the appliance in the sequence shown here. The ArcSight Storage Appliance can be reset to its initial condition, but other than that, several of the settings described here cannot be changed once set.



Make sure that you have obtained the license file from ArcSight Customer Support and installed it on your appliance.



One-time initialization can only be changed by performing a factory reset (see [Appendix C, Restoring Factory Settings, on page 55](#)). Be sure you know how you want the ArcSight Storage Appliance storage set up before performing the first steps of the initialization sequence (up to rebooting).

This sequence ensures that resources are created and parameters are set in the proper order:

- 1 [Define Storage Volume](#) - establish where ArcSight Storage Appliance stores event data

- 2 [Create Storage Groups](#) - apply retention policies to the Storage Volume
- 3 [Configure NTP](#) (optional, but strongly recommended)
- 4 [Configure Indexing](#)
- 5 [Reboot the Appliance](#) - commit the changes made in previous steps
- 6 [Create SmartMessage Receivers](#)

Define Storage Volume

Establish the ArcSight Storage Appliance's Storage Volume. See the section on Storage Volume in the *ArcSight Logger Administrator's Guide* for details. Choose **Local** to use Logger's built-in storage.

Pre-allocate 100% for your Storage Volume. Performance is degraded if you don't pre-allocate at least a portion of the storage volume.



Note

Storage Volume cannot be extended after initialization.

Create Storage Groups

Storage groups are used to support multiple retention policies that fit your requirements. The Default Storage Group has been pre-defined for you; you only need to configure its size. ArcSight recommends that you increase the maximum size of the Default Storage Group and increase the maximum age of the event retention policy to meet your internal data retention policy.

Following is an example of how you can use storage groups:

- Configure Default Storage Group.
 - ◆ Increase the maximum size to 500 GB (this can be increased in the future if needed).
 - ◆ Set the maximum age to 120 days.
- Create a second Storage Group with storage size of 5 GB and retention period set to 30 days.



Caution

Do not reboot the Appliance in the next step unless you are certain of your Storage Volume and Storage Group choices. Additional Storage Groups cannot be created once the Appliance is initialized.

See the section on Storage Groups in the *ArcSight Logger Administrator's Guide* for the details of adding Storage Groups.

Configure NTP

Configuring the Network Time protocol is optional, but a strongly recommended initialization step.

Precise time stamping of events is a key log management function. Therefore, ArcSight strongly recommends that you use Network Time Protocol (NTP) for system time instead of

manually configuring it. See the section on Time Settings in the *ArcSight Logger Administrator's Guide*.

Configure Indexing

The default option on the ArcSight Storage Appliance is No Indexing. However, ArcSight recommends using default indexing options for the storage appliance for better performance.

Reboot the Appliance

Reboot the storage appliance to commit changes before other resources can be created. See the section on System Reboot in the *ArcSight Logger Administrator's Guide*.



When the ArcSight Storage Appliance is rebooted, the Storage Volume and Storage Group settings become permanent. Only certain settings of non-default Storage Groups can be changed. See the *ArcSight Logger Administrator's Guide* for details on this.

Create SmartMessage Receivers

After initializing the storage, you can create a SmartMessage Receiver to listen for events. Make sure to use the settings mentioned below when creating the SmartMessage Receiver:

- Receiver Name: `esm-manager-receiver` (or any name of your choice)

Make sure to create a receiver on the ArcSight Storage Appliance. Also, make a note of the receiver name. You will be required to enter the receiver name when configuring the ArcSight Express Appliance. The receiver name you enter has to match the receiver name you configured on the ArcSight Storage Appliance exactly.

- Receiver Type: `SmartMessage`
- Receiver Encoding: `UTF-8`

After SmartMessage receiver is configured, enable the Receiver.

For more information about setting up the Receiver, see the *ArcSight Logger Administrator's Guide*.

Adding an ArcSight Storage Appliance

ArcSight Storage Appliance (Storage Appliance) is included with certain models of ArcSight Express. For those ArcSight Express models that do not include ArcSight Storage Appliance, you can purchase and install the Storage Appliance separately at a later time.

The ArcSight Express Storage Appliance is also known as ArcSight Logger when purchased separately.

See the *Getting Started with ArcSight Logger* document to install your newly purchased ArcSight Storage Appliance.

Once you have installed the ArcSight Storage Appliance, you will need to configure the ArcSight Forwarding Connector to send the events to the Storage Appliance. Refer to the sections, "Sending Events to ArcSight Logger" and "Forwarding Events to ArcSight Logger" in the *SmartConnector Configuration Guide for ArcSight Forwarding Connector* document available on the ArcSight Customer Support website.

Chapter 3

Configuring ArcSight Express Appliance

This chapter covers the following topics:

- [“Configuring ArcSight Express Appliance” on page 15](#)
- [“Configuring the Operating System” on page 15](#)
- [“Configuring Software Components on ArcSight Express Appliance” on page 20](#)
- [“The Next Steps” on page 23](#)

The steps in this chapter presume that you have performed the following:

- (If applicable) Installed the ArcSight Storage Appliance according to the instructions in the *Getting Started with ArcSight Logger* document available on ArcSight Customer Support download site, and followed the process in [Chapter 2, Configuring ArcSight Storage Appliance, on page 11](#).
- Installed the ArcSight Express Appliance according to the instructions in the *Getting Started with ArcSight Express* document that is included with ArcSight Express.
- Read the *ArcSight Express Release Notes*.

Configuring ArcSight Express Appliance

Configuring ArcSight Express Appliance is a two-step process:

- 1 Configuring the Red Hat Enterprise Linux (RHEL) operating system installed on the appliance.
- 2 Configuring the ArcSight Express software components that have been pre-installed on the appliance.

Both these are performed through the First Boot Wizard which starts automatically when you boot up the appliance for the first time.

Configuring the Operating System

The ArcSight Express 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 RHEL. 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**.
- 5 On the **ArcSight Password** panel, set up a password for the user **arcsight** (this user has already been created for you) and click **Forward**. Most components, including the Manager and ArcSight Web, run using an **arcsight** user account for security reasons.
- 6 On the **Oracle Password** panel, set up a password for the Oracle user **oracle** (this user has already been created for you) 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

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



Caution

Configure **eth0** only, and not any other port. ESM Manager will not communicate with the database if you configure ports other than eth0.

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

The Network Configuration panel appears.



For the Network Setup panels, 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.

- 8 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.



Caution

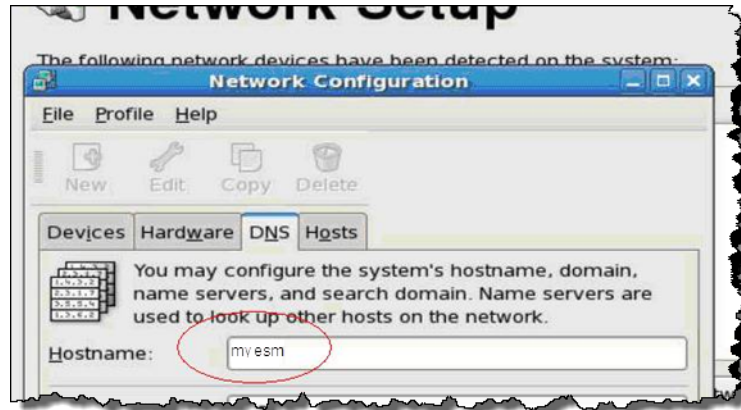
Make sure that the IP address you set up is available. The First Boot Wizard will report errors if the IP address has not been configured correctly.

- c Click **OK**.
- d For ports that will not be used, repeat from [Step 8](#) 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.

- 9 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). For example:



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.

Later, during the ESM Manager setup, you will be prompted to re-enter the hostname you use in the Network Setup panel.

- b Enter the IP address of your DNS server in the **Primary DNS** field.
 - c Click **OK**.
 - d Select **File->Save** to save your changes.
 - e Click **File->Quit** to exit the Network Configuration panel.
- 10** On the **Network Setup** panel, click **Forward**.
- 11** On the **Firewall** panel:
- a Select **Enabled** in the Firewall dropdown menu. Keep the listed trusted services selected.

Make sure the ports listed in the following note 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.

- b Click **Forward**.
- 12** 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 want to use. 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.



Note

If you entered the wrong server address and re-enter the correct address, it could take the appliance a few minutes to find the NTP server.

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.

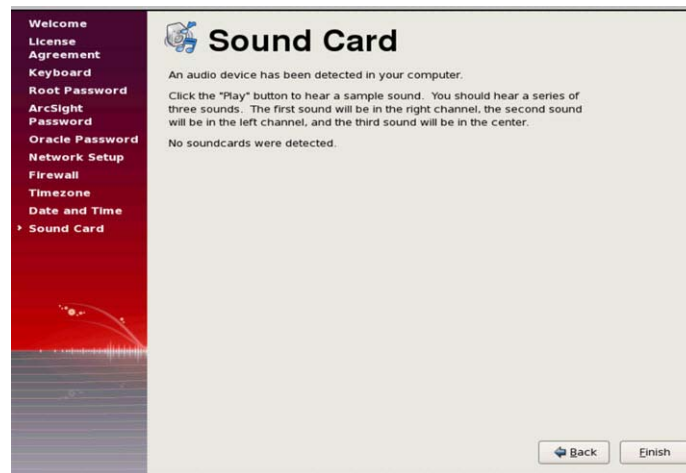
The list of servers configured by default points ArcSight Express to a virtual cluster of time servers operated by the NTP project. Assuming that UDP port 123 is open to the outside internet in your firewall, you can keep the default values, unless you would prefer to use your own cluster of NTP servers.



Note

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.

- 13 On the **Timezone** panel, select the Timezone in which your ArcSight Express ESM appliance is located and click **Forward**.
- 14 On the **Sound Card** panel, click **Finish**.



You are prompted to enter your username on the Red Hat Enterprise Linux 5 screen. This begins the second phase of the First Boot Wizard which will help you configure the pre-installed software components on your ArcSight Express appliance.

- 15 **Important!** Log in as user **root** and enter the password that you had set for this account in [Step 4 on page 16](#).

The next step is to set up the software components on the ArcSight Express Appliance.

After you have logged in successfully, the software components configuration wizard opens. Follow the directions in the [Configuring Software Components on ArcSight Express Appliance](#) section to configure ESM on ArcSight Express.

Configuring Software Components on ArcSight Express Appliance

After you have completed the OS configuration and logging in as root, you are now ready to configure the software components on ArcSight Express.

During this phase, the wizard prompts you for information required to configure the ArcSight Express software components - ArcSight Database, ArcSight Manager, ArcSight Web, and ArcSight Forwarding Connector.

See the *ArcSight ESM Installation and Configuration Guide* if you need further help with these panels. For more information on ArcSight Storage Appliance software, refer to *ArcSight Logger Administrator's Guide*. Download both these documents from the ArcSight Customer Support download site.



Restarting this wizard if you exit it...

If you exit out of any of the following panels, the wizard will exit with the following warning:

The wizard is not finished yet. Are you sure you want to exit?

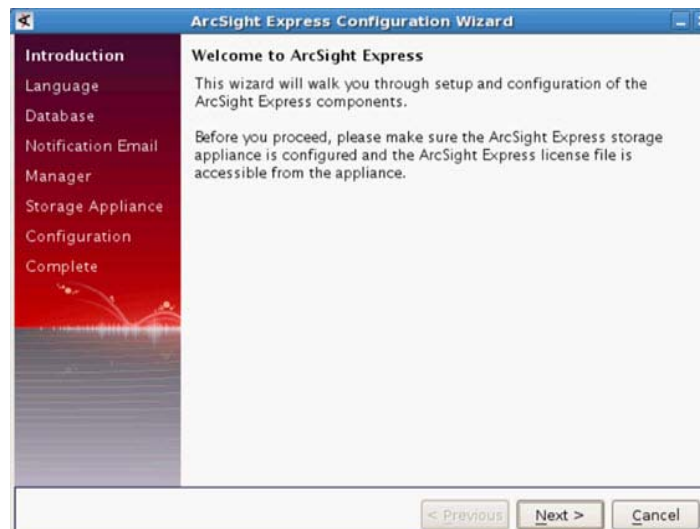
You can re-start the wizard at any point until you get to the panel which tells you that the Manager configuration has been complete. To re-start the wizard, run the following command from `/opt/arcsight/manager/bin` directory when logged in as user **root**:

```
./arcsight appliancefirstbootsetup
```

The wizard will open the panel you see in [Step 3](#) below.

The ArcSight Express Appliance is functional only after the successful completion of the wizard.

The wizard starts the next phase by displaying the Welcome panel that includes reminders about the storage appliance setup and the required access to the license file.



- 1 On the **Welcome** panel, click **Next**.
- 2 Select the language for the user interface display and click **Next**.
- 3 The database user account has already been created for you with username **arcsight**. On the Database Password panel, enter a password for this account and click **Next**.

- 4 On the **Oracle Passwords** panel, enter passwords for the SYS and SYSTEM accounts:

- ◆ **Oracle SYS Password**—Password for the Oracle superuser, SYS.
- ◆ **Oracle SYSTEM Password**—Password for the Oracle admin account.

Click **Next**.

- 5 On the **Notification E-mails** panel, configure the following e-mail addresses:

- ◆ **Notification e-mail address**—An e-mail address of the person who should receive e-mail notifications in the event that the ArcSight Manager goes down or encounters some other problem.
- ◆ **Escalation e-mail address**—An e-mail address of the person who should receive an escalation e-mail in case no action has been taken for a period of time after the notification e-mail was sent.
- ◆ **From Address**—E-mail address that will be used to represent the sender of the e-mail notifications.

Click **Next**.

- 6 On the **License File** panel, enter or navigate to the location where you have stored the ArcSight Express license file and click **Next**.

If you do not have a license file, contact ArcSight Customer Support to obtain one. Use the Web browser on the appliance to download the file once you obtain it from ArcSight Customer Support. Alternatively, download the license file elsewhere and use [scp](#) or [sftp](#) to get it onto the appliance.

- 7 On the Manager Information panel, enter the host name and login credentials for your ESM Manager administrator.

- ◆ **Manager host name**—Enter the host name of the appliance (IP address is also acceptable). Make sure your Manager host name matches the host name in the DNS tab as described in [Step 9 on page 17](#).
- ◆ **Administrator user name**—Enter the login name for the ESM Manager administrator.
- ◆ **Administrator password**—Enter the password to be used by the administrator.
- ◆ **Password confirmation**—Re-enter the password to confirm.

Click **Next**.

- 8 On the **Storage Appliance Option** panel, select **Forward events to ArcSight Storage Appliance**. This is the recommended setting. Click **Next**.



If you select the **Do not forward events to ArcSight Storage Appliance** option, you will not have any long term storage for your events. Skip the next step and go to [Step 10 on page 22](#) to begin the configuration process.

You also have the option to install and configure the ArcSight Storage Appliance at a later time. See ["Adding an ArcSight Storage Appliance" on page 13](#) for details on how to do this.



Make sure you have installed and configured ArcSight Storage Appliance and created a SmartMessage receiver on it before proceeding to the next step. Receivers are used to receive events from files and over the network. See the *ArcSight Logger Administrator's Guide* for details on how to create a SmartMessage receiver.

- 9 If you chose to forward events to the ArcSight Storage Appliance, enter the following information on the **Storage Appliance Parameters** panel:

- ◆ **ArcSight Storage Appliance host name**—The host name or IP address of the ArcSight Storage Appliance.
- ◆ **ArcSight Storage Appliance receiver name**—The name of the SmartMessage Receiver created on the ArcSight Storage Appliance.



The receiver name you enter in this field must exactly match the receiver name configured on the ArcSight Storage Appliance.

- ◆ **Forwarding Connector user name**—Enter a user name for creating an ArcSight Express account to be used by the Forwarding connector. This account is created under the admin folder in the Console. The Forwarding connector uses this account to pull events from the Manager, and forwards them to ArcSight Storage Appliance.
- ◆ **Forwarding Connector password**—Enter a password for the ArcSight Express account to be used by the Forwarding Connector. Re-enter it to confirm it.

Click **Next**.

A panel informs you that ArcSight Express is ready to be configured. The panel also displays a list of configuration tasks about to be performed.

- 10 Click **Next** to continue with the configuration.



Once the wizard has started configuring the software components, if you exit the wizard or if an error occurs, you will have to configure that component manually. See [Appendix A, Troubleshooting, on page 39](#) for detailed steps on how to do this.

You can see the progress and errors if any as the configuration process continues. Soon, the Tablespace Expansion Option panel displays a list of configuration tasks and the status of each, denoted either as Successful or Failed.

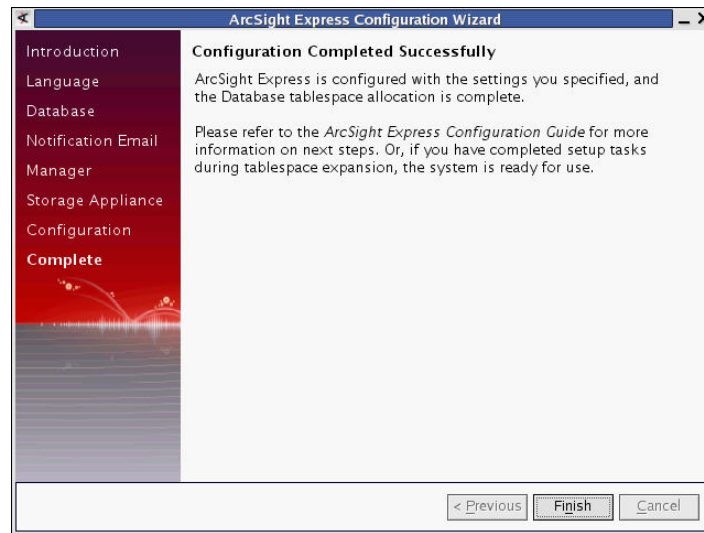


If you see a "Failed" status, or if you exit this wizard after it has started configuring the components but before successful completion of the wizard, you are required to manually configure the component that failed and perform the rest of the steps manually. See ["Failed" Status while Configuring or Starting a Component](#) section in the [Appendix A, Troubleshooting, on page 39](#) for detailed steps on how to do this. Optionally, you can restore your appliance to its original factory settings. See [Appendix C, Restoring Factory Settings, on page 55](#) for details.

- 11 On the **Tablespace Expansion Option** panel, click **Next**.

Allow time for table space expansion. You cannot restart the wizard once the Manager configuration has started.

A panel informs you about a successful configuration.



12 Click **Finish**.

ArcSight Express is ready for use.

The Next Steps

Now you have configured both the storage and ArcSight Express appliances. The next steps are:

- If there are any service packs available, be sure to download and install them. Refer to the respective service pack Upgrade Guide for instructions on how to upgrade ArcSight Express with the service pack.
- Download the ArcSight Console and install it on a supported platform. The Console should not be installed on ArcSight Express Appliance. Refer to the next chapter, [Installing ArcSight Console](#), for details on how to do this.

Also read the *ArcSight Express Release Notes*, available on the ArcSight Customer Support download site.

Chapter 4

Installing ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks on ArcSight Express, such as fine tuning the pre-installed ArcSight Express content and creating/editing/deleting users. The Console should only be used for administrative purposes. The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of ArcSight Web) to ArcSight Express. This chapter explains how to install and configure the ArcSight Console.



Note

Make sure that you have successfully configured the ArcSight Express appliance before proceeding.

The following topics are covered in this chapter:

[“Console Supported Platforms” on page 25](#)

[“Installing the Console” on page 26](#)

[“Starting the ArcSight Console” on page 32](#)

[“Reconnecting to the ArcSight Manager” on page 33](#)

[“Reconfiguring the ArcSight Console” on page 34](#)

[“Uninstalling the ArcSight Console” on page 34](#)

ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Express appliance.

Console Supported Platforms

The ArcSight Console is supported on the following operating systems.



Note

Refer to the ArcSight ESM Product Lifecycle document available on the ArcSight Customer Support website for the most current information on supported platforms.

Platform	Supported Operating System	Typical System Requirements
Linux	Red Hat Enterprise Linux (RHEL 5.4 and 5.5) Desktop 32-bit	x86-compatible multi-CPU system with 2-4 GB RAM

Platform	Supported Operating System	Typical System Requirements
Macintosh OS X	Macintosh OS X 10.6 64-bit	
Windows	Microsoft Windows 7 64-bit Microsoft Windows Vista SP2 64-bit Microsoft Windows XP Professional SP3 32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM

Installing the Console



Caution

Do not install the ArcSight Console on the ArcSight Express appliance. See the section [“Console Supported Platforms” on page 25](#) for supported platforms for ArcSight Console.



Note

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

Download the ArcSight Console installer file for your platform from the ArcSight Customer Support download site and install the Console on your system **after** configuring your appliance.

To install ArcSight Console, run the self-extracting archive file that is appropriate for your target platform. Go to the directory where the ArcSight Console Installer is located.

Platform	Installation File
Linux	ArcSight-5.0.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-5.0.x.nnnn.y-Console-Win.exe

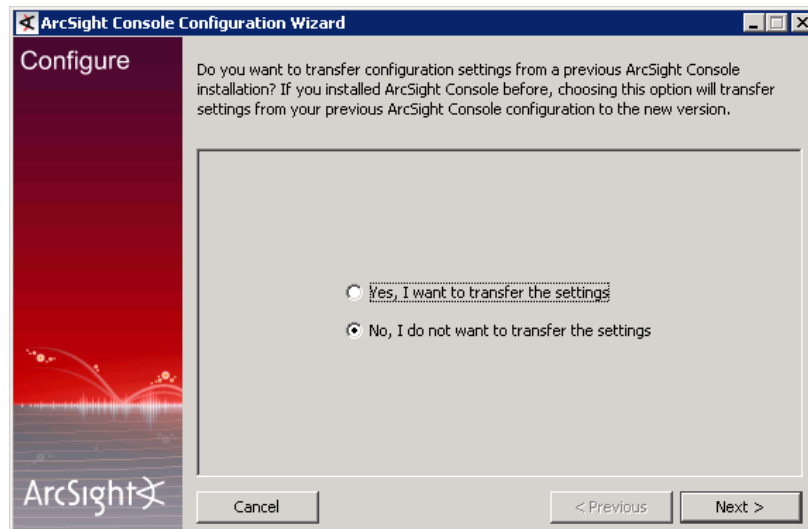
- 1 Click **Next** in the Installation Process Check screen.
- 2 Read the introductory text in the Introduction panel and click **Next**.
- 3 The “I accept the terms of the License Agreement” radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read the text click the “I accept the terms of the License Agreement” radio button and click **Next**.
- 4 Read the text in the Special Notice panel and click **Next**.
- 5 Navigate to an existing folder where you want to install the Console or accept the default and click **Next**. If you specify a folder that does not exist, the folder gets created for you.
- 6 Select where you would like to create a shortcut for the Console and click **Next**.

- 7 View the summary in the Pre-Installation Summary screen and click **Install** if you are satisfied with the paths listed. If you want to make any changes, use the Previous button to do so.

You can view the installation progress in the progress bar.

Transferring Configuration from an Existing Installation

After the Console has been installed, the wizard asks if you would like to transfer configuration options from an existing installation of ArcSight Console. Choose **No, I do not want to transfer the settings** to create a new, clean installation and click **Next**. If you choose **Yes, I want to transfer the settings**, the wizard will determine the version of the previous installation and may offer additional upgrade options.



Selecting the Mode in which to Configure ArcSight Console



The FIPS 140-2 mode is not supported on ArcSight Express appliance.

Next, you will see the following screen:



Select the **Run console in default mode** radio button and click **Next**.

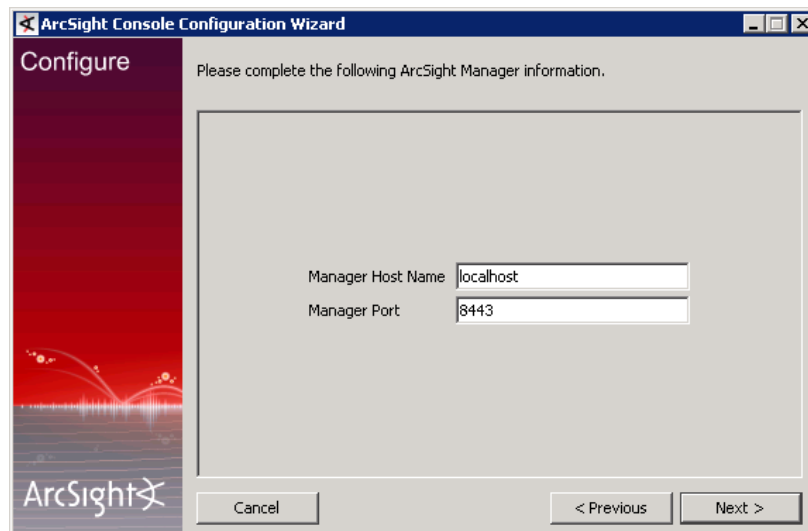
Manager Connection

The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. The hostname is the ArcSight Express appliance host name or its IP address. The Manager host name that you had entered in the First Boot Wizard while configuring the ArcSight Express appliance and the value of the Manager Host Name that you will be entering in this screen should be identical. If you had entered the machine name when configuring the First Boot Wizard, then you must enter the machine name here too, likewise, if you had entered the machine's IP address then you must enter the machine's IP address in this screen too.



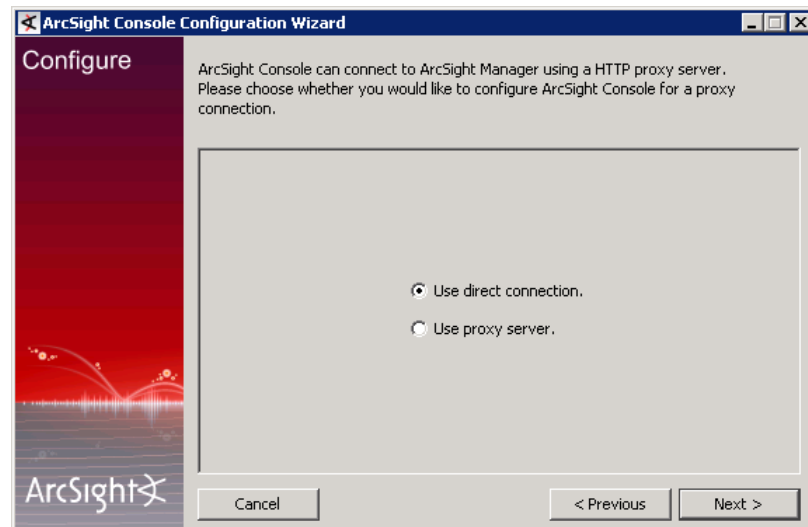
Do not change the Manager's port number.

Click **Next**.



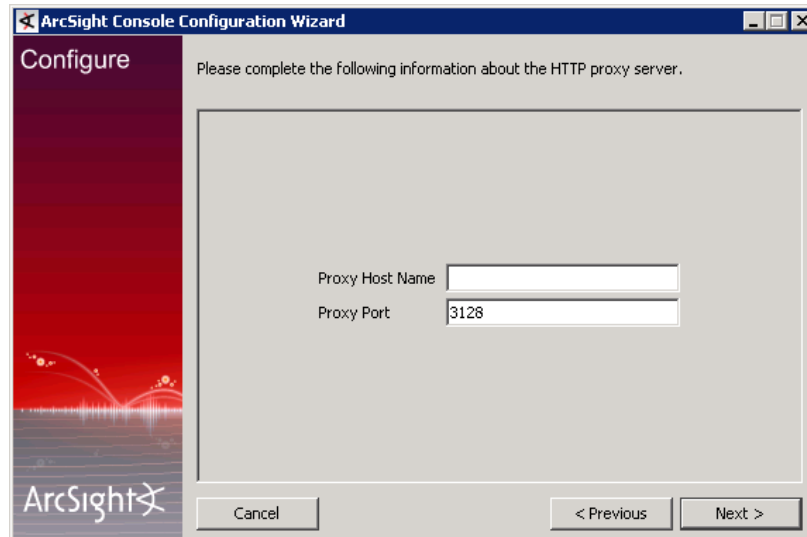
The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'Please complete the following ArcSight Manager information.' Below this text are two input fields: 'Manager Host Name' with the value 'localhost' and 'Manager Port' with the value '8443'. At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

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



The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'ArcSight Console can connect to ArcSight Manager using a HTTP proxy server. Please choose whether you would like to configure ArcSight Console for a proxy connection.' Below this text are two radio button options: 'Use direct connection.' (which is selected) and 'Use proxy server.'. At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

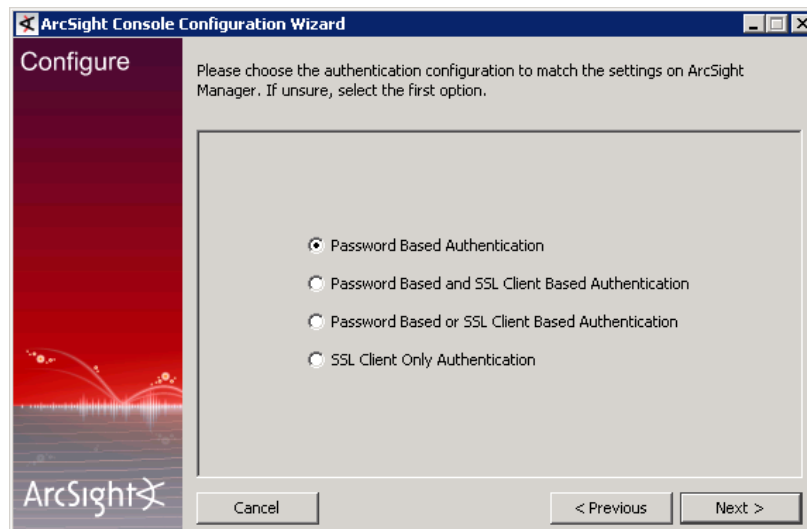


The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The title bar reads 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'Please complete the following information about the HTTP proxy server.' Below this text are two input fields: 'Proxy Host Name' and 'Proxy Port'. The 'Proxy Port' field contains the value '3128'. At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

Authentication

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



The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The title bar reads 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'Please choose the authentication configuration to match the settings on ArcSight Manager. If unsure, select the first option.' Below this text are four radio button options: 'Password Based Authentication' (selected), 'Password Based and SSL Client Based Authentication', 'Password Based or SSL Client Based Authentication', and 'SSL Client Only Authentication'. At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.



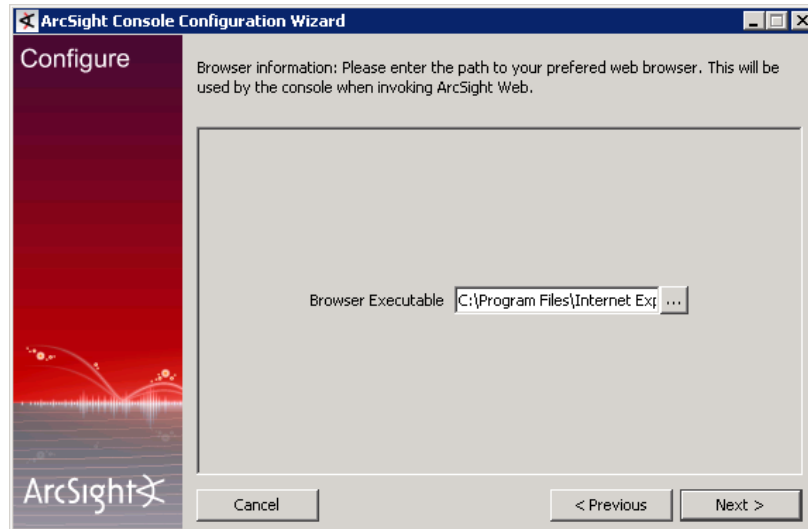
This release of ArcSight Express appliance supports **Password Based Authentication** only.

Select **Password Based Authentication** and click **Next**.

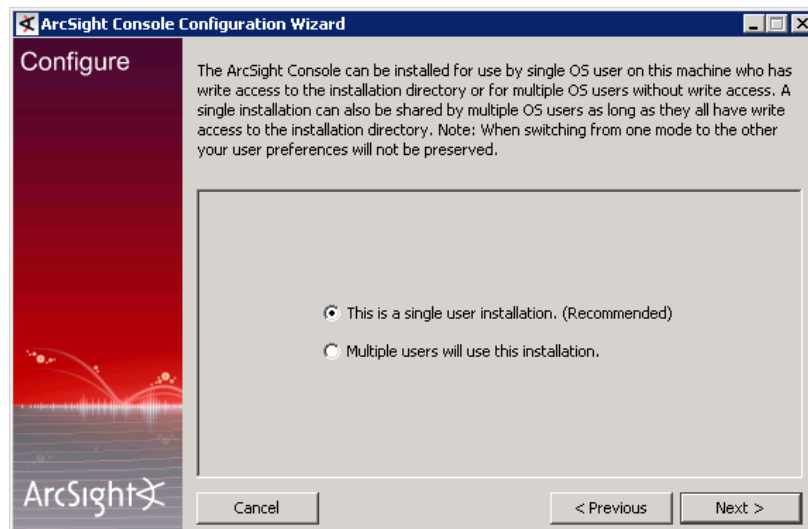
Web Browser

The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Base articles, and other web page content.

Specify the location of the executable for the web browser that you want to use to display the Knowledge Base articles and other web pages launched from the ArcSight Console. Click **Next**.

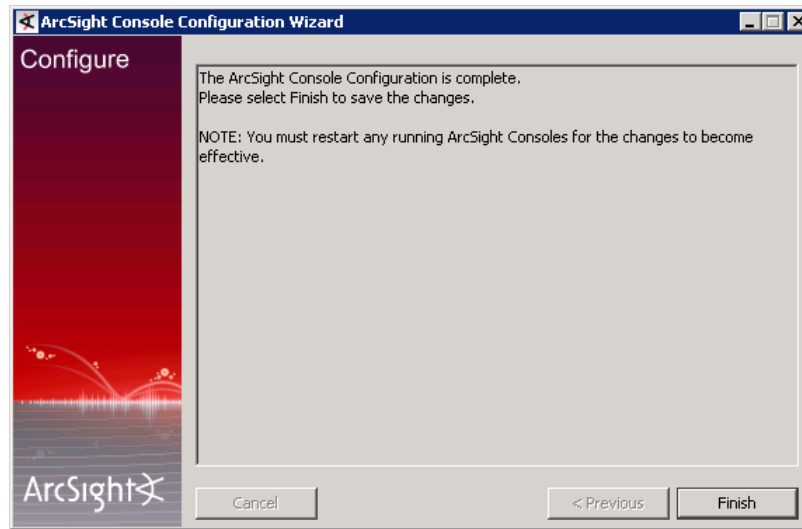


User Logs and Preferences



Select **This is a single user installation (Recommended)** and click **Next**.

You have completed configuring your ArcSight Console. Click **Finish** in the following screen.



Click **Done** in the next screen.

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

Starting the ArcSight Console



Note

The Manager on ArcSight Express Appliance should be up and running before you start the Console.

After installation and setup is complete, you can start ArcSight Console.

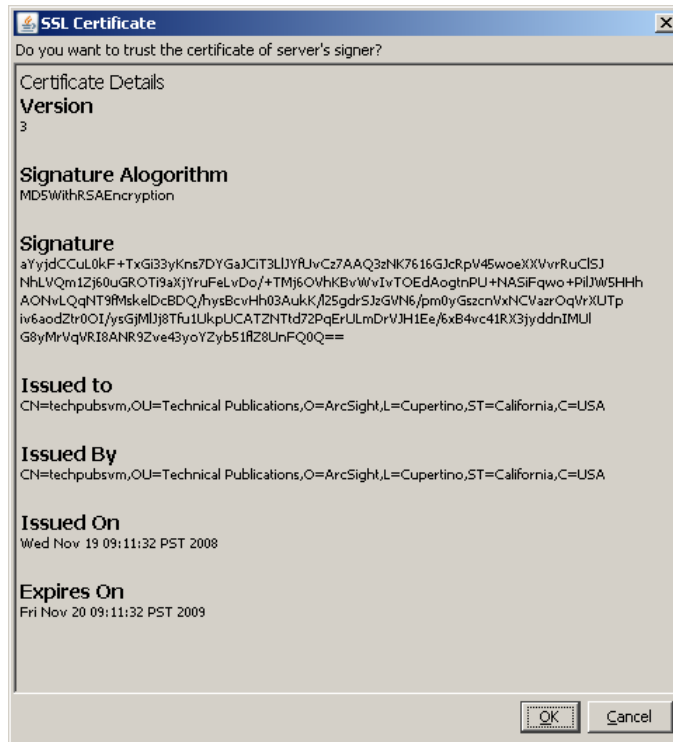
To start the ArcSight Console, use the shortcuts installed or open a command window on the Console's `\bin` directory and run:

```
arcsight console
```

Logging into the Console

To start the Console, click **Login**. When you start the Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the Manager's certificate. The prompt will show details specific to your settings (following is just an example). Click **OK** to trust the Manager's certificate. The certificate will be permanently

stored in the Console's truststore and you will not see the prompt again the next time you log in.



Creating ArcSight Express Users

The next step is to create users. ArcSight Express comes configured with a custom user group called ArcSight Express. Add users to this group with ArcSight Web privileges.

In the Navigator panel, go to **Users > Shared > Custom User Groups**. ArcSight Express comes configured with a custom user group called ArcSight Express. Add users to this group with ArcSight Web privileges.

- 1 In the Navigator panel, go to **Users > Shared > Custom User Groups**.
- 2 Right click on ArcSight Express and select **New User**.

For each user you add, provide a User ID and Password, and set the User Type to **Web User** and click **OK**. If the Navigator panel is not visible, you can open it by clicking Window->Navigator Panel. Then right click on **ArcSight Express** and select **New User**.

- 3 For each user you add, provide a User ID and Password, and set the User Type to **Web User** and click **OK**.

Reconnecting to the ArcSight Manager

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

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

exceptions during the Retry process while the connection is lost or ArcSight Manager is restarting.

Reconfiguring the ArcSight Console

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

```
arcsight consolesetup
```

and follow the prompts.

Uninstalling the ArcSight Console

Before uninstalling the ArcSight Console, exit the current session.

To uninstall on Windows, run the **Start->All Programs (Programs in the case of Windows XP)->ArcSight Console ->Uninstall ArcSight Console 5.0 SP1** program. If a shortcut to the Console was not installed on the Start menu, locate the Console's `\UninstallerData` folder and run:

```
Uninstall_ArcSight_Console.exe
```

Chapter 5

Using SmartConnectors with ArcSight Express

This chapter covers the following topics:

[“Installing the SmartConnector” on page 35](#)

[“Importing the Manager’s Certificate” on page 36](#)

SmartConnectors process raw data generated by various vendor devices throughout an enterprise. Devices are hardware and software products such as routers, anti-virus products, firewalls, intrusion detection systems (IDS), VPN systems, anti-DoS appliances, operating system logs, and other sources that detect and report security or audit information.

ArcSight SmartConnectors collect a vast amount of varying, heterogeneous information. Due to this variety of information, SmartConnectors format each event into a consistent, normalized *ArcSight events*, letting you find, sort, compare, and analyze all events using the same event fields. The “normalized” events are then sent to the ArcSight Manager and are stored in the ArcSight Database or forwarded to ArcSight Storage Appliance if you choose to enable forwarding events.

You have the option to use up to four SmartConnector(s) locally depending on available resources on the ArcSight Storage Appliance.

Installing the SmartConnector

Installing and configuring the SmartConnector is a three step process:

- 1 Install the SmartConnector.

For an overview of the SmartConnector installation and configuration process, see the *SmartConnector User’s Guide*.

- 2 Import the Manager’s certificate to the Connector’s truststore. See the section [Importing the Manager’s Certificate](#) for details on how to do this.

- 3 Configure the SmartConnector.

For complete configuration instructions for a particular SmartConnector, see the configuration guide for that connector. The product-specific configuration guide provides specific device configuration information, installation parameters, and device event mappings to ArcSight ESM fields.

Importing the Manager's Certificate

You will be required to import the Manager's certificate manually. You can use either of the two methods to import the certificate:

- Use the [keytoolgui](#) tool. See the *ArcSight ESM Administrator's Guide* for details on importing the Manager's certificate using the [keytoolgui](#).
- Import the Manager's certificate using the Connector Manager software.

Using keytoolgui to Import the Manager's Certificate

You will need to export the Manager's certificate from ArcSight Express Appliance before you can import it on the Smart Connector in the Smart Connector server.

Exporting the Manager's Certificate

To export the Manager's certificate:

- 1 Open a shell/command prompt window on the ArcSight Express Appliance.
- 2 Log in as the user **arcsight** and run the following command from the ArcSight Express Manager's `/opt/arcsight/manager/bin` directory:

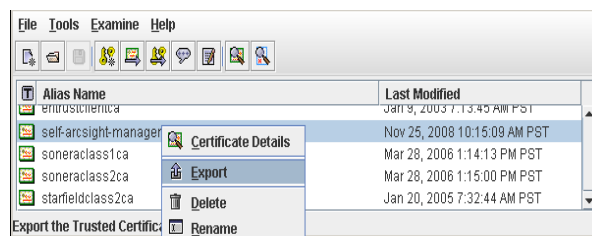
```
./arcsight keytoolgui
```

The keytoolgui interface opens.

- 3 Select **File->Open KeyStore** from the menu and navigate to the Manager's truststore (`cacerts`) located in `/opt/arcsight/manager/jre/lib/security/` directory.



- 4 Enter the keystore password. The default password is **changeit**.
- 5 Right-click the Manager's certificate as shown below and select **Export**.



- 6 Accept the default settings in the **Export Type** dialog and click **OK**.
- 7 Navigate to the location where you want to export the certificate and make sure to enter `cacerts` in the File Name text box when naming the certificate. Click **Export**.

A prompt informs you that the export is successful.

- 8 Click **OK** and exit the [keytoolgui](#).
- 9 Transfer (or scp) this exported certificate file from the ArcSight Express Appliance to the Smart Connector server where you will be importing it into the SmartConnector.

Importing the Manager's Certificate into the SmartConnector's Truststore

Import the certificate you exported above into the Connector's truststore.

To import the Manager's certificate:

- 1 Open a shell/command prompt window on the SmartConnector server.
- 2 Log in as the user **arcsight** and run the following command from the Connector's `/opt/arcsight/connector/current/bin` directory:

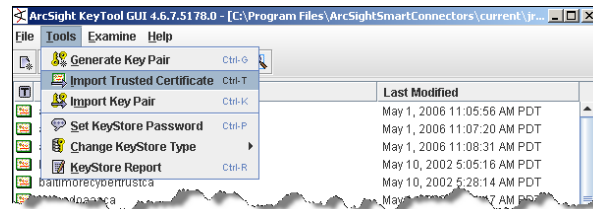
```
./arcsight agent keytoolgui
```

The keytoolgui interface opens.

- 3 Select **File->Open KeyStore** from the menu and navigate to the Connector's truststore (`cacerts`) located in the `/opt/arcsight/connector/current/jre/lib/security/` directory.



- 4 Enter the password. The default password is **changeit**.
- 5 Click **Tools->Import Trusted Certificate**.



- 6 Navigate to the Manager's certificate, select it, and click **Import**.
- 7 At the prompt, click **OK** to see the certificate details.
- 8 On the **Certificate Details** dialog, click **OK** to accept the certificate.
- 9 At the prompt, click **Yes** to accept the certificate as trusted.
- 10 On the **Trusted Certificate Entry Alias** dialog, enter an alias for the certificate and click **OK**.

A message informs you that the import is successful.

- 11 Click **OK** to dismiss the message.
- 12 Click **File->Save KeyStore** to save the certificate in the Connector's truststore and exit the `keytoolgui` interface.

Import the Manager's certificate using the Connector Manager

- 1 Copy the `cacerts` file manually from the ArcSight Express Manager's `/opt/arcsight/manager/jre/lib/security/` directory on to your local desktop.
- 2 Open a web browser on your desktop and connect to the ArcSight Storage Appliance by typing the URL in the following format:

`https://<the_IP_address_of_your_ArcSight_Storage_Appliance>`
- 3 To upload the `cacerts` file to the ArcSight Storage Appliance, go to **Configuration->Advanced Operations->CA Certs->CA Certs Repositories** tab and click **Upload**.
- 4 Navigate to the file, select the file, and click **Submit** to start the upload process.
- 5 Click **Apply CA Certs** tab and select the container by checking the checkbox to the right of it.
- 6 Click **Update** to apply this `cacerts` to the container.
- 7 Continue to configure the connectors and register them with the Manager whose certificate you just imported.

Appendix A

Troubleshooting

The following information may help solve problems that might occur when installing or using ArcSight Express. In some cases, the solution can be found here or in other ArcSight Express documentation, but ArcSight Customer Support is available if you need it. Refer to the documents listed in section [“Related Documents” on page 9](#).

This chapter covers the following topics:

- [“Location of Log files for Components” on page 39](#)
- [“Customizing ESM Components Further” on page 40](#)
- [“Fatal Error when Running the First Boot Wizard” on page 41](#)
- [“Manager Service Failed when Starting” on page 42](#)
- [““Failed” Status while Configuring or Starting a Component” on page 42](#)

If you intend to have ArcSight Customer Support guide you through a diagnostic process, prepare to provide specific symptoms and configuration information.

Location of Log files for Components

The log file for each component can be found in the following location:

On the ArcSight Express Appliance:

First Boot Wizard:

- `/opt/arcsight/manager/logs/firstboot.log`
- `/opt/arcsight/manager/logs/default/managerwizard.log`
- `/opt/arcsight/manager/logs/default/serverwizard.log`

ArcSight Database:

- `/opt/arcsight/db/logs`

ArcSight Manager:

- `/opt/arcsight/manager/logs/default`

ArcSight Web:

- `/opt/arcsight/web/logs/default`

ArcSight Forwarding Connector:

```
/opt/arcsight/connector/current/logs
```

On the ArcSight Storage Appliance:

ArcSight Logger:

```
/opt/arcsight/logger/logs
```

On the machine where you install the Console:

ArcSight Console:

```
<ARCSIGHT_HOME>\current\logs
```

Customizing ESM Components Further

The First Boot Wizard configures the software components on the ArcSight Express Appliance (ArcSight Database, ArcSight Manager, ArcSight Web, and ArcSight Forwarding Connector) for you. But, in the event that you would like to customize a component further, you can follow these instructions to start the setup program for the component:

ArcSight Database

While logged in as **root**, run the following command from `/opt/arcsight/db/bin` directory:

```
./arcsight database pc
```

ArcSight Manager

While logged in as **arcsight**, run the following command from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

ArcSight Web

While logged in as **arcsight**, run the following command from `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

Follow the prompts on the wizard screens. To get more information on an individual screen for any of the components listed above, see the *ArcSight ESM Installation and Configuration Guide* available on the ArcSight Customer Support download site.

ArcSight Forwarding Connector

While logged in as **root**, run the setup program from the `/opt/arcsight/connector/current/bin` directory:

```
./arcsight connectorsetup
```

and follow the prompts on the screen. Refer to the *SmartConnector Configuration Guide for ArcSight Forwarding Connector* document available on the ArcSight Customer Support download site.

Fatal Error when Running the First Boot Wizard

If you encounter a fatal error such as the one shown below while running the First Boot Wizard, the wizard will display an error message and then exit.



To resolve this issue, try the following steps:

- 1 Check the `/opt/arcsight/manager/logs/firstboot.log` file to figure out where the error occurred.
- 2 Verify that the IP address for the appliance has been configured correctly (eth0 has been configured correctly) and is available (not already in use for some other system on your network).
- 3 Make sure that the tnslister and Oracle services are started.

To check the status of the TNS listener, run this command as **oracle** from the `/opt/arcsight/db/bin` directory:



Note

To run the commands in this step, you must be logged in as the Oracle user. Run the following command to switch to the Oracle user if not logged in as one already:

```
su - oracle
```

```
% ./arcdbutil lsnrctl status
```

To check whether Oracle services have been started, run the following commands:

```
% ./arcdbutil sql
```

```
Enter user-name: / as sysdba
```

```
Enter password:
```

Enter **arcsight** when prompted for the password. You will get the sqlplus prompt only if the Oracle services are running.

- 4 Restart the First Boot Wizard by running the following command from the `/opt/arcsight/manager/bin` directory when logged in as **root**:

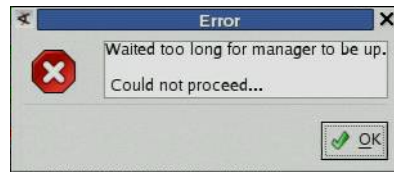
```
./arcsight appliancefirstbootsetup
```

The First Boot Wizard can only be rerun until the point that the Manager has not been configured.

If the steps above do not solve the issue, you will be required to revert your ArcSight Express Appliance to its factory settings. For instructions on how to do this, see [Appendix C, Restoring Factory Settings, on page 55](#).

Manager Service Failed when Starting

If the Manager service fails to start and displays the following error:

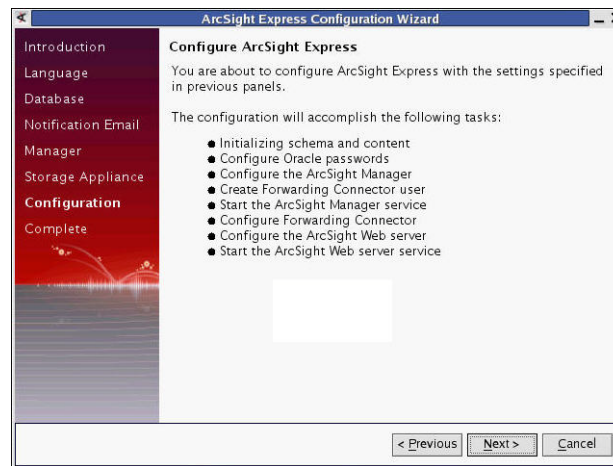


- Start the Manager service manually. See [Step 3 on page 43](#) for details.
- Configure the Forwarding Connector and ArcSight Web manually. See [“Failed” Status while Configuring or Starting a Component](#) section for details.
- Run the tablespace expansion manually. See [Step 2 on page 43](#) for details.

In the event that any of the above steps do not work, we recommend that you revert your ArcSight Express Appliance to its factory settings. For instructions on how to do this, see [Appendix C, Restoring Factory Settings, on page 55](#).

“Failed” Status while Configuring or Starting a Component

If you cancel out of the First Boot Wizard before you begin configuring ArcSight Express, you can re-run the wizard.



However, once the configuration begins, if any step fails or you cancel out of the wizard, you must then run the corresponding component setup program and configure the component manually.

If you see a “Failed” status for any component, such as the following example, you must then configure the component manually. To find out the reason for the failure, look at the log for the component. See [“Location of Log files for Components” on page 39](#) for the location of the logs.



Following are the steps to configure a component manually:

- 1 To configure the partition management notification e-mails for the ArcSight Database software component, run the following command from `/opt/arcsight/db/bin` directory on ArcSight Express Appliance while logged in as **root**:

```
./arcsight database pc
```

and follow the prompts on the screen. Refer to the *ArcSight ESM Installation and Configuration Guide* for information on each screen. You can download this guide from the ArcSight Customer Support download site.

- 2 To expand the tablespaces manually, run the following command from `/opt/arcsight/db/bin` directory on ArcSight Express Appliance while logged in as **root**:

```
./arcsight database xts
```

- 3 To start the Manager service manually, run the following command from `/etc/init.d` directory as **root** on ArcSight Express Appliance:

```
./arcsight_manager start
```

and follow the prompts on the screen. Refer to the *ArcSight ESM Installation and Configuration Guide* for information on each screen.

- 4 To configure the Forwarding Connector manually, run the setup program from the `/opt/arcsight/connector/current/bin` directory on ArcSight Express Appliance as **root**:

```
./arcsight connectorsetup
```

and follow the prompts on the screen. Refer to the *SmartConnector Configuration Guide for ArcSight Forwarding Connector* document available on the ArcSight Customer Support download site.

- 5 To configure ArcSight Web manually, run the following command from the `/opt/arcsight/web/bin` directory on ArcSight Express Appliance as **arcsight**:

```
./arcsight websetup
```

and follow the prompts on the screen. Refer to the *ArcSight ESM Installation and Configuration Guide* for information on each screen.

- 6 To start the Web server service manually, run the following command from `/etc/init.d` directory as **root** on ArcSight Express Appliance:

```
./arcsight_web start
```

- 7 To manually start a Forwarding Connector service, run the following command from `/etc/init.d` directory on ArcSight Express Appliance as **root**:

```
./arc_logger_connector start
```

In the event that any of the above steps do not work, we recommend that you revert your ArcSight Express Appliance to its factory settings. For instructions on how to do this, see [Appendix C, Restoring Factory Settings, on page 55](#).

Changing the IP Address of the ArcSight Express Appliance After Configuring It in the First Boot Wizard

You set the IP address for the ArcSight Express Appliance when you boot the appliance for the very first time and configure it using the First Boot Wizard. Once the First Boot Wizard has run successfully, you will not be allowed to run it again. In case you want to change the IP address of the ArcSight Express Appliance after running the First Boot Wizard successfully, follow these steps:



Note

- Manager and Web setup commands must be run when logged in as user **arcsight**.
- All other commands must be run as user **root**.
- All services are to be stopped and started when logged in as user **root**.

- 1 Stop all ESM related services:
 - a To stop the Manager service, run the following command from `/etc/init.d` directory as **root**:


```
./arcsight_manager stop
```
 - b To stop the Web service, run the following command from `/etc/init.d` directory as **root**:


```
./arcsight_web stop
```
 - c To stop the Forwarding Connector service, run the following command from `/etc/init.d` directory as **root**:


```
./arc_logger_connector stop
```
- 2 Stop the TNS Listener by running the following command from `/opt/arcsight/db/bin` directory:


```
./arcdbutil listener stop
```
- 3 Change the IP address of the appliance in the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.
- 4 Change the IP address in the `/home/oracle/OraHome11g/network/admin/sqlnet.ora` file.
- 5 Reboot the ArcSight Express ESM appliance.

Only if you had entered an IP address (instead of a host name) do the following additional steps:

When prompted for a Manager Host Name in the First Boot Wizard, then do the following additional steps:

- 6 Stop the Manager and Web services again. These services would have started upon reboot.
- 7 Run the following to start the setup program for the Manager from `/opt/arcsight/manager/bin` directory:


```
./arcsight managersetup
```

This opens the Manager's setup wizard.

- a** Enter the new IP address that you had set for your appliance in [Step 4](#) above in the Manager Host Name field when prompted by the wizard.
 - b** Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new IP address.
- 8** Start the Manager service by running the following command from the `/etc/init.d` directory as **root**:

```
./arcsight_manager start
```

- 9 Import the Manager's newly generated self-signed certificate on the webserver using the `keytoolgui` tool. See ["Using keytoolgui to Import the Manager's Certificate" on page 36](#).
- 10 While logged in as user **arcsight**, run the following to start the setup program for the Web from the `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

- a** Enter the new IP address in Webserver Host Name field when prompted.
 - b** Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new IP address.
- 11** If you chose to set up Logger and Forwarding Connector when configuring your appliance using the First Boot Wizard, stop the Forwarding Connector service by running the following command from the `/etc/init.d` directory as **root**:

```
./arc logger connector stop
```

- 12 Import the Manager's certificate on the connector using [keytoolgui](#). See *ArcSight ESM Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

- 13** Run the setup program for the connector from the `/opt/arcsight/connector/current/bin` directory:

```
./arcsight connectorsetup
```

and enter the new IP address for the appliance in the Host Name field when prompted.

- 14** Restart the Connector service by running the following from the `/etc/init.d` directory as **root**:

```
./arc_logger_connector start
```

- 15 Import the Manager's certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the keytoolgui. See *ArcSight ESM Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

- 16** Test to make sure that the clients can connect to the Manager.

Changing the Host Name of the ArcSight Express Appliance After Configuring It in the First Boot Wizard



Note

- Manager and Web setup commands must be run when logged in as user **arcsight**.
- All other commands must be run as user **root**.
- All services are to be stopped and started when logged in as user **root**.

You set the host name for the ArcSight Express Appliance when you boot the appliance for the first time and configure it using the First Boot Wizard. Once the First Boot Wizard has run successfully, you will not be allowed to run it again. In case you want to change the host name of the ArcSight Express Appliance after running the First Boot Wizard successfully, follow these steps:

- 1 Stop all ESM related services:
 - a To stop the Manager service, run the following command from `/etc/init.d` directory as **root**:

```
./arcsight_manager stop
```
 - b To stop the Web service, run the following command from the `/etc/init.d` directory as **root**:

```
./arcsight_web stop
```
 - c To stop the Forwarding Connector service, run the following command from the `/etc/init.d` directory as **root**:

```
./arc_logger_connector stop
```
- 2 Stop the TNS Listener by running the following command from the `/opt/arcsight/db/bin` directory:

```
./arcdbutil listener stop
```
- 3 Change the host name of the appliance by editing it in the `/etc/sysconfig/network` file.
- 4 Edit the `/etc/hosts` file to reflect the new host name of the ArcSight Express Appliance.
- 5 Run the following from the shell prompt to change the hostname on the appliance:

```
hostname <new_hostname>
```
- 6 Run the following from a shell prompt for your changes to take effect:

```
service network restart
```
- 7 Change the host name in the `/home/oracle/OraHome11g/network/admin/listener.ora` file.
- 8 Change the host name in the `/home/oracle/OraHome11g/network/admin/tnsnames.ora` file.
- 9 Change the host name in the `/home/oracle/OraHome11g/network/admin/sqlnet.ora` file.

- 10** Start the TNS Listener by running the following command from `/opt/arcsight/db/bin` directory:

```
./arcdbutil listener start
```

- 11** Start the Partition Configuration wizard by running the following command from `/opt/arcsight/db/bin` directory:

```
./arcsight database pc
```

and enter the new host name in the Database Host Name field when prompted.

If you had entered an IP address in the Manager Host Name field when configuring the ArcSight Express Appliance you will also need to do the following steps:

- 12** Start the Manager by running the following command from the `/etc/init.d` directory as **root**:

```
./arcsight_manager start
```

- 13** Start the Web by running the following command from the `/etc/init.d` directory as **root**:

```
./arcsight_web start
```

If you had entered a host name when prompted for a Manager Host Name in the First Boot Wizard, then you will be required to do the following in addition to the steps mentioned above:

- 14** Stop the Manager.

- 15** Run the Manager's setup program from the `/opt/arcsight/manager/bin` directory as **arcsight**:

```
./arcsight managersetup
```

- a** Enter the new host name that you set for your appliance in the Manager Host Name field when prompted by the wizard.
- b** Make sure to select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new host name.

- 16** Start the Manager service by running the following command from the `/etc/init.d` directory as **root**:

```
./arcsight_manager start
```

- 17** Import the Manager's newly generated self-signed certificate on the Webserver using the `keytoolgui` tool. See *ArcSight ESM Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

- 18** While logged in as **arcsight**, run the following to start the setup program for the Web from the `/opt/arcsight/web/bin` directory:

```
./arcsight websetup
```

- a** Enter the new host name in the Manager Host Name and the Webserver Host Name fields when prompted.

- 19** If you had chosen to set up Logger and Forwarding Connector when configuring your appliance using the First Boot Wizard, stop the Forwarding Connector service by running the following command from the `/etc/init.d` directory as user **root**:

```
./arc_logger_connector stop
```

- 20** Import the Manager's certificate on the connector using `keytoolgui`. See *ArcSight ESM Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

- 21** While logged in as **root**, run the setup program for the connector from the `/opt/arcsight/connector/current/bin` directory:

```
./arcsight connectorsetup
```

and enter the new host name for the appliance in the Host Name field when prompted.

- 22** Restart the Connector service by running the following from the `/etc/init.d` directory as **root**:

```
./arc_logger_connector start
```

- 23** Import the Manager's certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the `keytoolgui`. See *ArcSight ESM Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

- 24** Test to make sure that the clients can connect to the Manager.

Default Settings for Components

This appendix provides the default settings for each software component in ArcSight Express. It covers the default settings for the following:

[“General” on page 49](#)
[“ArcSight Database” on page 49](#)
[“ArcSight Manager” on page 51](#)
[“About ArcSight Web” on page 52](#)
[“ArcSight Forwarding Connector” on page 52](#)
[“ArcSight Logger” on page 53](#)

You can always customize any component by running its setup program. Refer to [Appendix A, Troubleshooting, on page 39](#) for information on running the setup program for a component.

The following tables list the default settings for each component.

General

Setting	Default Value
default password for Java keystore	changeit

ArcSight Database

The ArcSight Express Appliance comes pre-installed with Oracle 11g. An Oracle instance has already been created for you. The following are some of the default values that have been pre-configured in ArcSight Database for you:

Setting	Default Value
ArcSight Database Home	/opt/arcsight/db
Oracle Home	/home/oracle/OraHome11g
Location of Oracle data files	/opt/data
Space allocated	1344 GB
Remaining free space	245 GB

Setting	Default Value
Allocated memory	20 GB
Tablespace name	Data file size
ARC_SYSTEM_DATA	5 GB (1 file x 5 GB)
ARC_SYSTEM_INDEX	5 GB (1 file x 5 GB)
ARC_EVENT_DATA	425 GB (25 files x 17 GB)
ARC_EVENT_INDEX	850 GB (50 files x 17 GB)
ARC_UNDO	96 GB (12 files x 8GB)
ARC_TEMP	48 GB (6 files x 8GB)
Partition Retention Method	Space Based Retention
Target free space %	15%
Partition Management runtimes	Runs 4 times in a 24 hour period. The default timings are 02:00, 07:00, 13:00, 20:00.
E-mail notification level	Warning
Location of Control Files	/home/oracle/OraHome11g/oradata/arc sight
Database Host name	Host name or IP address of your ArcSight Express ESM machine
Database port number	1521
Database instance name	arcsight
Database OS user name	oracle
Database user name (This account will be used by ArcSight Manager to connect to ArcSight Database)	arcsight
Database Template Size	XXLarge
Database Character set	UTF-8
Allowed TNS Clients	localhost
Auto Archive Redo logs	No
Database OS username	oracle
System User name	systemuser
Minimum Partition Retention Period	2 days by default. To increase this period, add the following property in the /opt/arcsight/manager/config/server.properties file: sbr.extend.min.retention.period=

About Data Retention on ArcSight Express

ArcSight Express uses the Space Based Retention method to maintain online data. Your data is retained based on the target free space which is the amount (percentage) of free space available in your database. The target free space is set to 15% by default. You can change this percentage by running the `./arcsight database pc` command from the `/opt/arcsight/db/bin` directory and entering the desired percentage when prompted.

The Partition Manager (a component of the ArcSight Manager that manages the life-cycle of event data partitions from creation to elimination) is scheduled to run once every 6 hours. When the Partition Manager runs, it calculates the free space in the database. If you get sudden spikes of events that fill up the database before the next 6-hourly scheduled run of the Partition Manager, you will get alerts in the Console and via e-mail. You can either manually launch Partition Manager to free up space immediately or just wait for the next scheduled Partition Manager run to do so. (In the latter case, events would continue to be cached on the connectors.) As soon as it detects that the free space available is less than the target free space, it drops the oldest retained partition and continues to drop the next oldest partition until the available free space reaches the target free space percent. At a minimum the current partition plus the two most recent partitions are retained even if the amount of free space in the database falls below the target free space. For example, if today is Wednesday, the Partition Manager makes sure to at least retain partitions from Monday and Tuesday even though that might mean leaving less than the target free space in the database. Audit events are generated every time a partition is dropped.

For long term data storage beyond what the disk space on ArcSight Express Appliance allows, forward the events to ArcSight Storage Appliance.

ArcSight Manager



ArcSight Manager uses a self-signed certificate, which gets generated for you when you configure the appliance using the First Boot Wizard. When you log into the Console for the very first time you will be prompted to accept the Manager's certificate. You can either click Yes in that dialog or optionally import the Manager's certificate manually at a later time.

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

Setting	Default Value
Location of Manager	<code>/opt/arcsight/manager</code>
Manager host name	Host name or IP address of ArcSight Express
Manager Port	<code>8443</code>
Manager license file	Obtain from ArcSight Customer Support
Packages installed	ArcSight Express, ArcSight Administration
Java Heap Memory	3072 MB
Authentication Type	Password Based
Type of certificate used	self-signed
Default password for keystore	<code>password</code>

Setting	Default Value
Default password for truststore	changeit
E-mail Notification	Internal SMTP server. If you want to use an External SMTP server, run the following command from the /opt/arcsight/manager/bin directory and set up the external SMTP server when prompted: ./arcsight managersetup
Sensor Asset Auto Creation	Enabled
Packages/default content installed	Appliance-related content
Manager installed as service	Yes (name of service is arcsight_manager)

About ArcSight Web

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

Setting	Default Value
Location of ArcSight Web	/opt/arcsight/web
ArcSight Web host name	Host name or IP address of ArcSight Express
ArcSight Web port	9443
Java Heap Size	512 MB
Authentication Type	Password Based
Default password for keystore	password
Default password for truststore	changeit
ArcSight Web installed as service	Yes (name of service is arcsight_web)

ArcSight Forwarding Connector

The Forwarding Connector receives the events from the Manager and forwards the events to the ArcSight Storage Appliance using the SmartReceiver. The following are some of the default values that have been pre-configured in ArcSight Web for you:

Setting	Default Value
Location of ArcSight Forwarding Connector	/opt/arcsight/connector
ArcSight Forwarding Connector installed as service	Yes
Name of the Forwarding Connector Service	arc_logger_connector

ArcSight Logger

The ArcSight Storage Appliance includes the ArcSight Logger software, software for connector management and 4 connectors that run on the appliance itself.

Setting	Default Value
ArcSight Logger host name	IP address of ArcSight Logger
ArcSight Logger Port	443

Appendix C

Restoring Factory Settings

ArcSight Express 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 Express to factory settings will permanently delete all event data and configuration settings.

To restore ArcSight Express to its original factory settings, perform these steps:

- 1 Attach a keyboard, monitor, and mouse directly to the ArcSight Express system.
- 2 Reboot ArcSight Express 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.



- 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. Click **Back** to revisit previous pages and make changes as required.



Do not interrupt or power-down the ArcSight Express appliance during the restore process. Interrupting the restore process can force the system into a state from which it cannot recover.

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.

Index

A

- ArcSight
 - Database 6
 - Manager 6
 - Web 6
- ArcSight Console 7, 25
 - connecting to the Manager 28
 - installing 25, 26
 - reconfiguring 34
 - reconnecting to Manager 33
 - starting 32
 - uninstalling 34
 - user logs and preferences 31
 - web browser configuration 31
- ArcSight Database 6
 - default settings 49
 - setup 40
- ArcSight Express 5
 - appliance 5
 - changing host name after it has been configured 46
 - changing IP address after configuring it 44
 - communication overview 8
 - configuring 15
 - configuring software components 20
 - customizing components 40
 - data retention 51
 - deployment overview 7
 - effects of communication when components fail 8
 - Logger 5, 6
 - pre-installed software 5
 - related documents 9
 - restarting wizard 20
 - Restore Factory Settings 55
 - storage appliance 5
 - using smartconnectors 11, 35
- ArcSight Express Appliance
 - configuring 15
- ArcSight Express Storage Appliance
 - configuring 11
- ArcSight Forwarding Connector 6
 - default settings 52
 - setup 40
- ArcSight Logger
 - default settings 53
- ArcSight Manager 6
 - default settings 51
 - setup 40
 - transferring configuration 27
- ArcSight Web 6
 - default settings 52
 - setup 40

C

- changing
 - host name of ArcSight Express 46
 - IP address of ArcSight Express Appliance 44
- configuring
 - ArcSight Express Appliance 15
 - ArcSight Express Storage Appliance 11
 - RHEL 15
 - software components on ArcSight Express 20
 - web browser in Console 31
- connecting
 - ArcSight Console to Manager 28
- Console
 - installing 26
 - supported platforms 25
- customizing
 - components on ArcSight Express 40

D

- data retention
 - ArcSight Express 51
- database 6
- default settings
 - ArcSight Database 49
 - ArcSight Forwarding Connector 52
 - ArcSight Logger 53
 - ArcSight Manager 51
 - ArcSight Web 52

F

- factory settings
 - restore 55
- First Boot Wizard
 - fatal error 41

I

- installing
 - ArcSight Console 25, 26

L

- Logger 5
 - configuring 11

M

- Manager 6

O

- overview
 - ArcSight Express communication 8
 - ArcSight Express deployment 7

P

- preferences
 - ArcSight Console 31
- Pre-installed software
 - ArcSight Express 5

R

- reconfiguring
 - ArcSight Console 34
- reconnecting
 - Console to Manager 33
- restarting
 - ArcSight Express wizard 20
- RHEL, configuring 15

S

- setup
 - ArcSight Database 40
 - ArcSight Forwarding Connector 40

- ArcSight Manager 40
- ArcSight Web 40
- space based retention 51
- starting
 - ArcSight Console 32
- supported platforms
 - Console 25

T

- Troubleshooting 39
 - Failed status 42
 - fatal error 41
 - Manager service failed 42

U

- uninstalling
 - ArcSight Console 34
- user logs
 - ArcSight Console 31

W

- Web 6
- Web browser
 - configuring in Console 31