Configuration Guide

ArcSight Express All-in-One™
Version 2.0

Includes
ArcSight Express™ v5.0 SP1 Patch 1
ArcSight Logger™ v5.1 GA

August 2011

ArcSight™
An HP Company

Configuration Guide ArcSight Express All-in-One™

Revision History

Date	Product Version	Description
8/12/2011	ArcSight Express version 2.0 (with ArcSight Express v5.0 SP1 Patch 1 and ArcSight Logger v5.1 GA)	ArcSight Express version 2.0

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://www.arcsight.com/supportportal
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

What is ArcSight Express All-in-One™?

ArcSight Express All-in-One™ 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 ArcSight Logger as storage component within a single appliance. The ArcSight Express All-in-One appliance 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 All-in-One

ArcSight Express All-in-One is pre-installed with the following software components:

- ArcSight Manager™
- ArcSight Database
- ArcSight Web™
- ArcSight Forwarding Connector
- ArcSight Logger™ and two default containers, each one supporting four connectors to total eight connectors
- ArcSight TRM™ (Threat Response Manager)
- ArcSight IdentityView™ Express
- ArcSight SmartConnector™ for Microsoft Active Directory Actor Model Info

ArcSight Console™ (also called ESM Console) is installed on a separate system.

Check the ArcSight Download Center for the availability of upgrades to ArcSight Express All-in-One components.

ArcSight Manager™

ArcSight Manager is at the center of ArcSight Express All-in-One. ArcSight Manager is the server that receives event data from SmartConnectors, and correlates and stores them in the database. ArcSight Manager also provides advanced correlation and reporting capabilities. The ArcSight Web interface is used to retrieve this information from ArcSight Manager and display it.

ArcSight Database

ArcSight Database is the central repository for all information collected by 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 All-in-One. ArcSight Web is a web server component that enables you to access ESM Manager securely using a browser. ArcSight Web supports the following browsers on the Windows Vista or Windows XP platforms:

- Internet Explorer 6 and 7
- Firefox 2.0 - 3.0

Check the Product Lifecycle document available on the ArcSight Customer Support website for updated 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 ArcSight Manager.

ArcSight Logger™

ArcSight Logger is a log management solution that is optimized for extremely high event throughput. Logger stores time-stamped text messages and 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 user interface in Logger 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 various destinations. ArcSight Express All-in-One™ supports a total of eight SmartConnectors (four per container).

ArcSight Forwarding Connector

The ArcSight Forwarding Connector is a component that transports events from ArcSight Manager to a destination, in this case, to the Logger component in the appliance.

ArcSight Threat Response Management

The ArcSight Threat Response Management (TRM) component enables you to respond quickly to cyber-security incidents detected on the network.

ArcSight IdentityView™ Express

ArcSight IdentityView is a solution that provides Privileged User and Shared Account monitoring capabilities. IdentityView works with Microsoft Active Directory for user management.

ArcSightSmartConnector™ for Microsoft Active Directory Actor Model

This ArcSightSmartConnector extracts the user identity information from an IDM database and populates the Actors resource in ArcSight's Console with this data. The Actors lists are populated and updated dynamically as changes are made in Active Directory.

ArcSight Console™

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

Deployment Overview

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

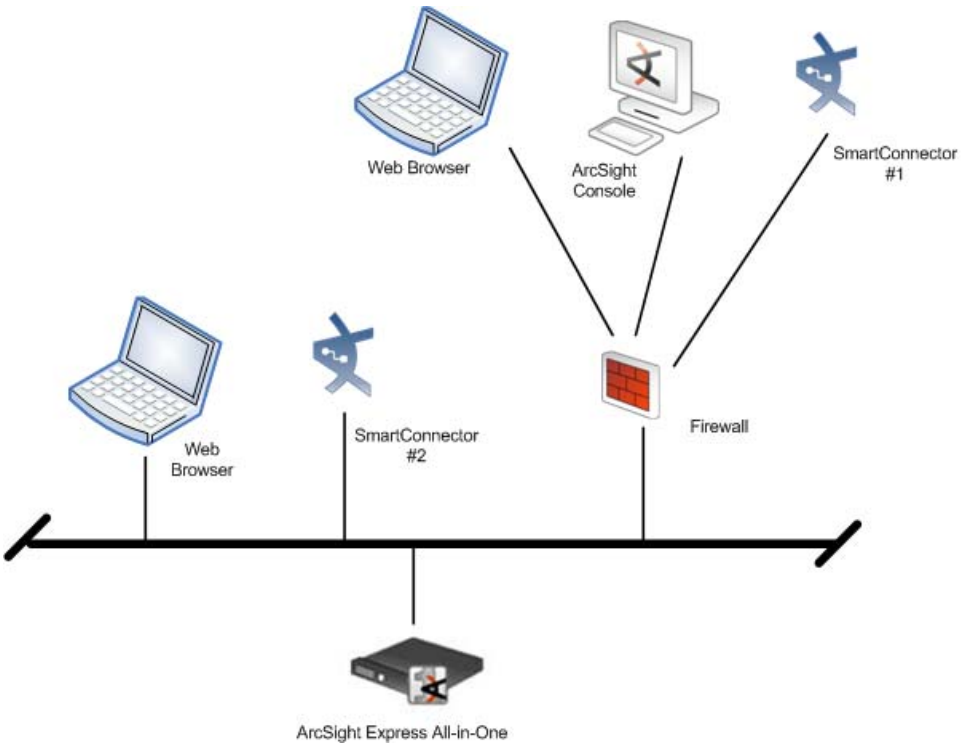


Figure 1-1 ArcSight Express All-in-One™ Deployment Overview

ArcSight Express All-in-One Communication Overview

ArcSight Console, ArcSight Manager, and ArcSightSmartConnector 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.

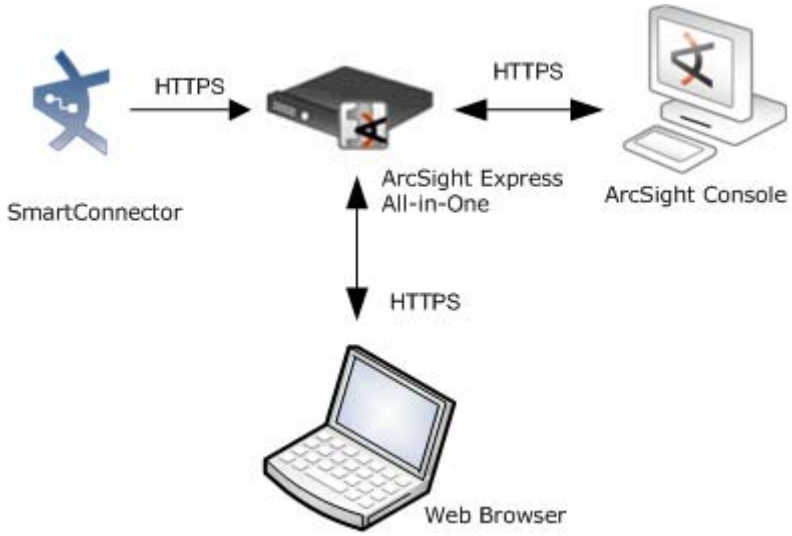


Figure 1-2 ArcSight Express All-in-One™ Solution - Communication Overview

SSL works over TCP (Transport Control Protocol) connections. The default incoming TCP ports are as follows:

- ArcSight Manager = 8443
- ArcSight Web = 9443
- ArcSight Logger = 443
- ArcSight TRM = 1443

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

Effect on Communication if Components Fail

As the illustration shows, events are collected by one or more SmartConnectors and sent to ArcSight ESM. From ArcSight ESM, the Forwarding Connector sends these events to Logger for storage.

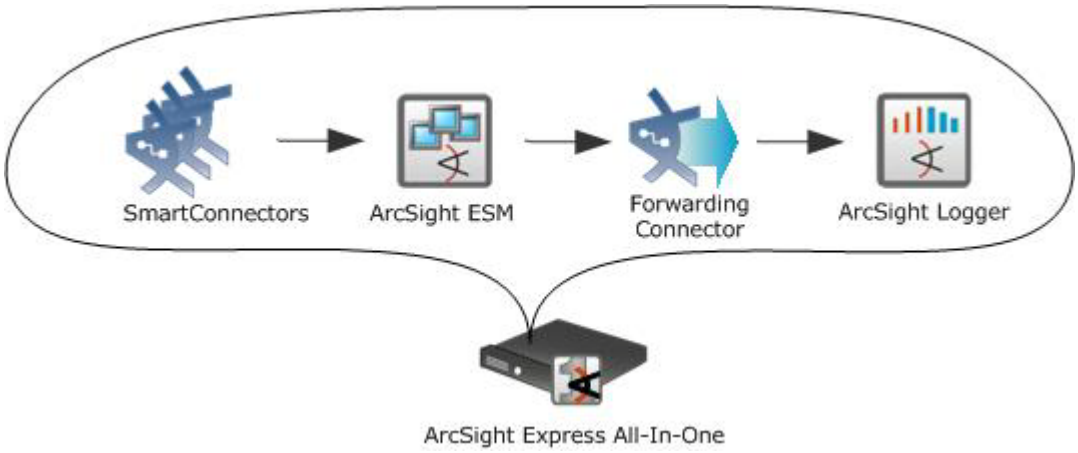


Figure 1-3 ArcSight Express All-in-One™ Event Flow

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

If the database is unavailable for any reason, such as when the database is filled to capacity, ArcSight 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 Manager is unavailable, the SmartConnectors start caching events to prevent loss of event data. The database server becomes 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, Manager will continue to store the events in its file store which is 10 GB in size. If the file store fills up, Manager will start dropping the oldest events and the newer events will continue to get stored on the file store.

If Logger fails, the Forwarding Connector will cache the events that were supposed to be forwarded to the database.

Related Documents

To get you started, the *Getting Started with ArcSight Express All-in-One™* document is available in hard copy and is packaged with the ArcSight Express All-in-One appliance. The ESM User's Guide online help (Console Help) is available from ArcSight Console, which is installed in a separate system.

In addition to this Configuration Guide, you can download and refer to the following documents from the ArcSight Download Center.

Important: If you are referring to the individual documents listed here, realize that the ArcSight software components in ArcSight Express All-in-One™ can also be purchased individually in their own appliances. For purposes of ArcSight Express All-in-One™, the setup is different than that for individual appliances. You should first refer to this Configuration Guide for setup guidelines, then refer to specific topics in the other documents when this guide directs you to do so.

For ArcSight Express All-in-One:

- *Getting Started with ArcSight Express All-in-One™*
- *ArcSight Express All-in-One™ Release Notes*
- *ArcSight Express Content User's Guide*

For ArcSight Manager:

- *ArcSight ESM Administrator's Guide*
- *ArcSight ESM Release Notes*
- *ArcSight ESM User's Guide or Console Help*

For ArcSight Logger and Connector Management:

- *ArcSight Logger Administrator's Guide*
- *SmartConnector User's Guide*
- *ArcSight Connector Appliance Administrator's Guide*
- *ArcSight Connector Appliance Release Notes*

For ArcSight Forwarding Connector:

SmartConnector Configuration Guide for ArcSight Forwarding Connector

For ArcSight TRM:

- *ArcSight NSP Installation and Administration Guide*

  Refer to the Threat Response Management chapter.
- *ArcSight NSP Release Notes*
- *SmartConnector Configuration Guide for ArcSight Threat Response Manager*

For ArcSight IdentityView and Active Directory Model Import Connector:

- *ArcSight Deployment Guide, IdentityView Express*
- *ArcSight IdentityView Express Release Notes*
- *ArcSight SmartConnector Configuration Guide for Microsoft Active Directory Actor Model*
- *Release Notes, SmartConnector for Microsoft Active Directory Actor Model*
- *ArcSight Solution Guide, IdentityView*

Chapter 2

Configuring ArcSight Express All-in-One

This chapter covers the following topics:

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

- Completed ArcSight Express All-in-One installation by following the instructions in *Getting Started with ArcSight Express All-in-One*. Read the *ArcSight Express All-in-One Release Notes* before proceeding.
- Obtained the required license from ArcSight Customer Support and followed instructions on where to store the file. This single file is good for all software components in the appliance.

Configuration Overview

Configuring ArcSight Express All-in-One includes the following process:

1. Obtaining the License File
2. Configuring the Red Hat Enterprise Linux (RHEL) operating system installed on the appliance (Configuring the Operating System)
3. Configuring ArcSight ESM (includes Database, Manager, and Web) using First Boot Wizard (Configuring the Operating System)
4. Copying the CA Certs file to connector directories (Copying the CA Certs File)
5. Configuring ArcSight Logger (Initializing ArcSight Logger)
6. Configuring the ArcSight Forwarding Connector (Configuring ArcSight Forwarding Connector)
7. Configuring optional software components.

ArcSight Express All-in-One is composed of multiple ArcSight software components and each component comes with its own set of documents. Those documents reflect the component's installation and use as standalone products and provide a level of detail not covered in this chapter. The procedures in this chapter will direct you to the applicable ArcSight document at the appropriate stage of the configuration. However, due to specific requirements of ArcSight Express All-in-One, you may be asked to change the sequence of some standard setup steps, or use settings specific to ArcSight Express All-in-One. These exceptions will be pointed out to you as required.

Obtaining the License File

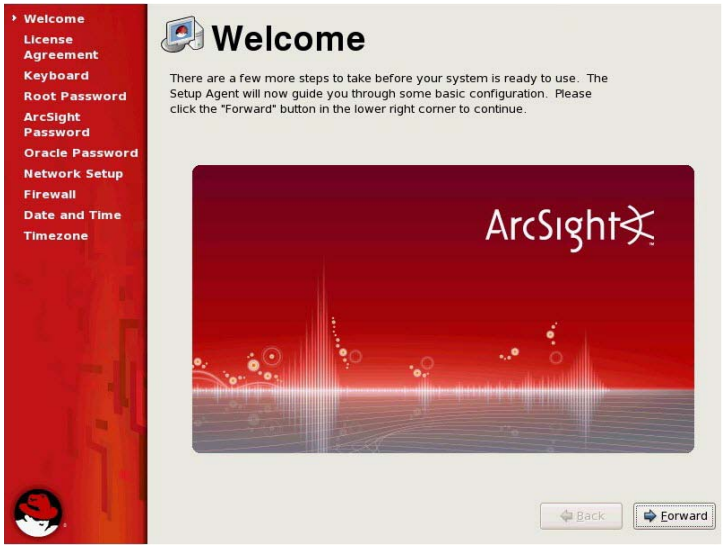
Make sure you have the license file for the ArcSight Express All-in-One appliance. You will be required to specify this license file during the configuration process.

If you do not have a license file, contact ArcSight Customer Support. You can use the Web browser on the appliance to download the file once you obtain it from ArcSight Customer Support. Alternatively, you can download the license file elsewhere and use `scp` or `sftp` to access the appliance.

Configuring the Operating System

ArcSight Express All-in-One 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 following 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. Click **Yes, I agree to the License Agreement** and click **Forward**.
3. On the Keyboard panel, choose the appropriate keyboard for your locale and click **Forward**.
4. On the Root Password panel, enter a password for the root account used for system administration. Re-enter to confirm it and click **Forward**.
5. On the ArcSight Password panel, enter a password for the default user account called *arcsight* (this user has already been created for you). Use any password you want, then click **Forward**.

   The *arcsight* user account is required to run ESM components, such as the Manager and ArcSight Web.
6. On the Oracle Password panel, set up a password for the Oracle user called *oracle* (this user has already been created for you) and click **Forward**.

   The next step is to configure the IP address 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.

Configure **eth0** only, and not any other port. ArcSight Manager will not communicate with the database if you configure ports other than eth0. The remaining ethernet ports are disabled by default.

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

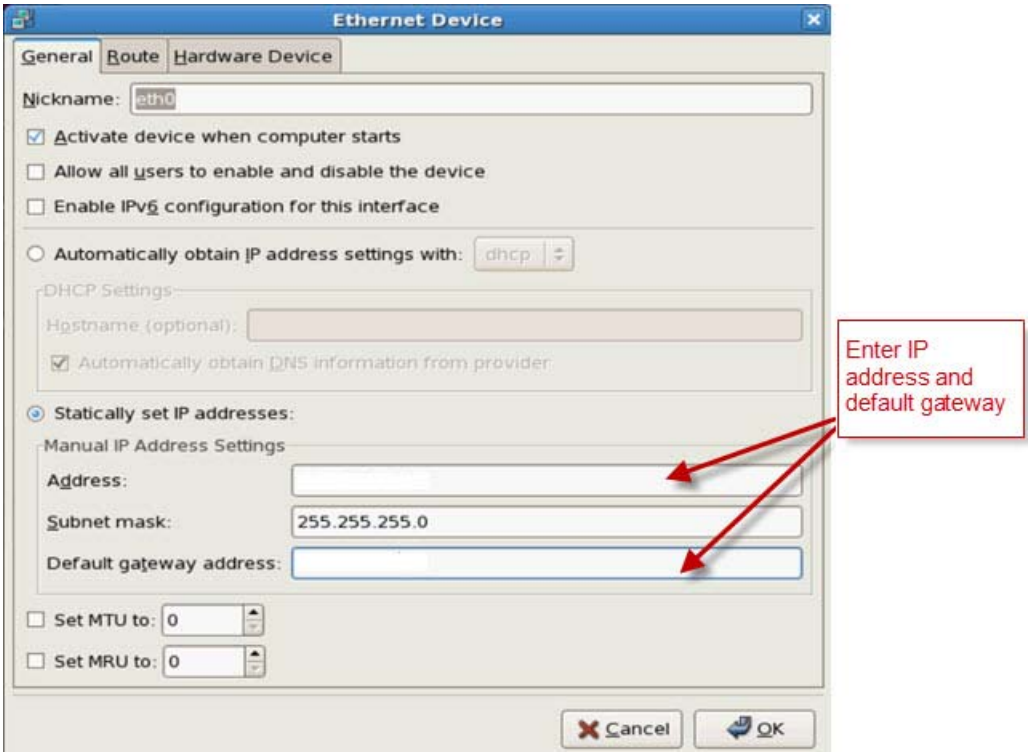
The Network Configuration panel appears.

> **Note** 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. Click **Activate device when computer starts**.

b Set the IP address, subnet mask, and default gateway.



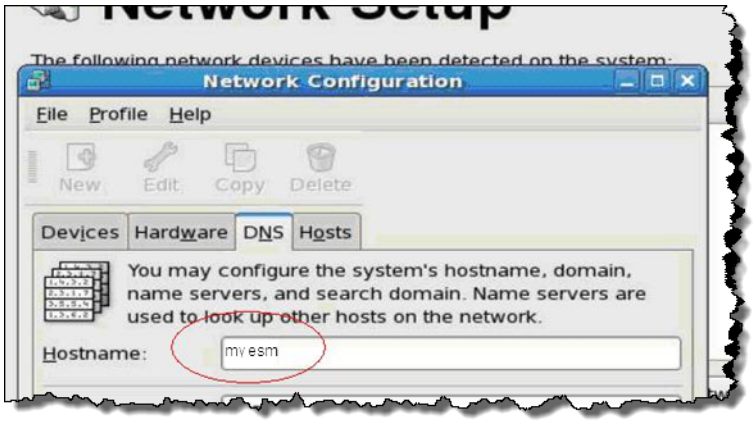
> **Caution** Make sure that the IP address you set up is available and not being used by another system. The First Boot Wizard will report errors if the IP address has not been configured correctly.

c Click **OK**.

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 the hostname you want to use can be resolved by your name server. Enter your preferred 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 ArcSight Manager setup, you will be prompted to re-enter the same hostname as entered here.

b Enter the IP address of your DNS server in the **Primary DNS** field.

c Click **OK**.

d Choose **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 Choose **Disabled** in the Firewall dropdown menu. Click **Yes** to confirm.

Make sure the ports listed below are open:

- 8443 used by ArcSight Manager for communication
- 9443 used by ArcSight Web for communication
- 22 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.

If you entered the wrong server address and then correct it, the appliance could take 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 All-in-One 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.

13 On the Timezone panel, select the Timezone in which your ArcSight Express All-in-One appliance is located.

14 Click **Finish**.

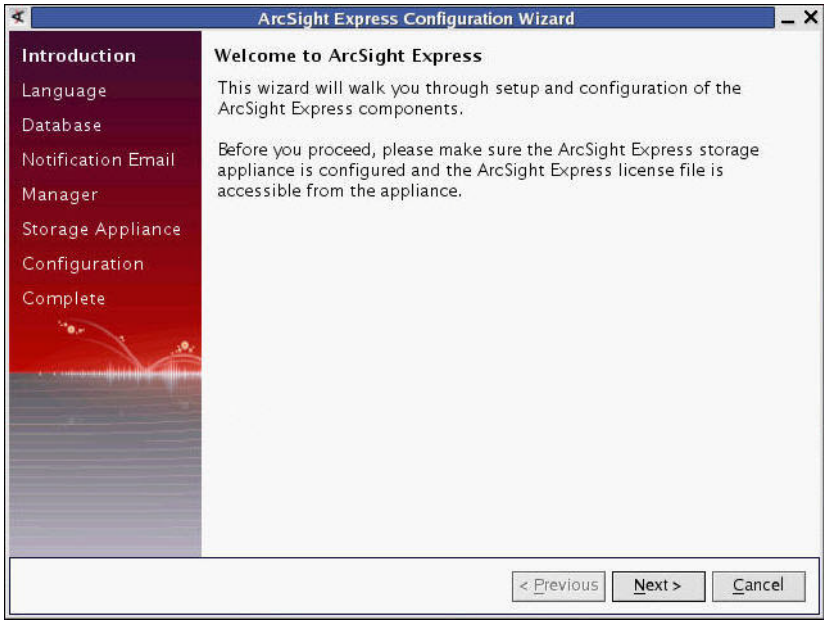
You are prompted to enter your username on the Red Hat Enterprise Linux 5 screen. This begins the second phase of the First Boot Wizard which will help you configure ArcSight ESM.

15 **Important!** Log in as **root** and enter the password that you had set for this account in Step 4 on page 17.

After you have logged in successfully, the ArcSight Express Configuration Wizard opens. Follow the directions in the Configuring ArcSight ESM™ section to continue with the next phase.

Configuring ArcSight ESM™

After you have completed the OS configuration and have logged in as root, you are now ready to configure the software components on the appliance. The wizard continues from the operating system setup to the following pane:



At this stage of the setup, you will configure ArcSight ESM which includes ArcSight Manager, ArcSight Database, and ArcSight Web.

Restarting this wizard if you exit it...

If you exit any of the screens, 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 screen which tells you that the Manager configuration has been completed. To re-start the wizard, run the following command as **root** from the directory, `/opt/arcsight/manager/bin`:

```
./arcsight appliancefirstbootsetup
```

The wizard will open the screen you see in Step 1 below.

ArcSight Express All-in-One is functional only after the successful completion of the wizard.

1. On the first screen after logging in as root, the wizard reminds you to configure the Storage Appliance before configuring ArcSight Express All-in-One. Ignore this reminder (you will set up Logger later) and click **Next**.
2. Choose the language for the user interface display and click **Next**.
3. The database user account has already been created for you with the username **arcsight**. Enter a password for this account and click **Next**.
4. On the Oracle Passwords panel, enter passwords (enter twice to confirm) for the SYS and SYSTEM accounts:
   - **Oracle SYS Password**—Password for the Oracle superuser, SYS.

- **Oracle SYSTEM Password**—Password for the Oracle admin account.

Do not use the $ character when specifying a password for the database user 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.

The license file is applicable to all software components bundled in ArcSight Express All-in-One. If you are referring to the individual documents about these components and a separate licensing requirement is mentioned, note that those licenses apply only if the software components are purchased individually.

Click **Next**.

7 On the Manager Information panel, enter the host name and login credentials for your ArcSight 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 a on page 19. The Manager host name setting will be used to generate a self-signed certificate and also when the Console connects to the Manager.
- **Administrator user name**—Enter the login name for the ArcSight 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, choose **Do not forward events to ArcSight Storage Appliance**. Choose this setting because ArcSight Logger is not yet configured.

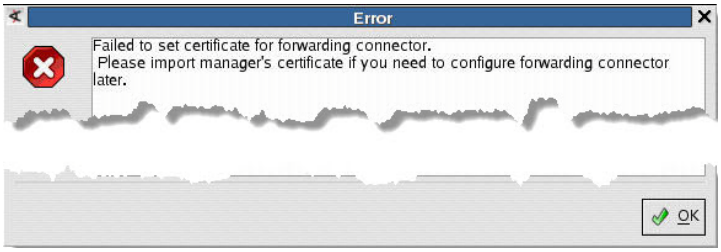
ArcSight Storage Appliance (Logger) configuration will take place later.

9 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.

During the configuration process, the following informational message appears:



This error message is expected because the option to forward events to the storage appliance was not selected in Step 8 above.

Ignore this message and click **OK** to close the dialog.

11 Click **Next** to continue with the configuration.

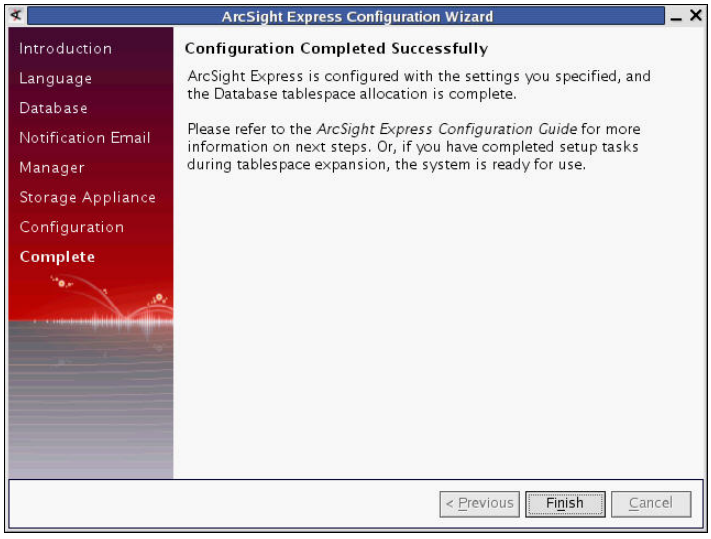
As the configuration process continues, you can see the progress and errors if any. Soon, the Tablespace Expansion Option panel displays a list of configuration tasks and the status of each, expressed either as Successful or Failed.

Caution If you see a "Failed" status on any listed task, or if you exit this wizard while it is still configuring the components, you are required to manually configure the failed component and manually perform the rest of the steps. See "Failed" Status While Configuring or Starting a Component section in the Appendix A, Troubleshooting, on page 53 for detailed steps on how to do this.

12 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.



13 Click **Finish**.

Proceed to Copying the CA Certs File.

Copying the CA Certs File

The following procedure will help you copy the CA Certs file to the different Connector directories and specify **arcsight** as the owner of the directories. A script is provided to accomplish this task.

To copy the CA Certs file:

1 Run the following command:

```
/root/bin/addCerts.sh
```

Do not copy CA Certs into the onboard Logger connector directory which is in `/opt/arcsight/connector`. This connector is for connecting to an external ArcSight ESM installation and is not configured for ArcSight Express All-in-One use. Doing so will result in an infinite loop.

2 Change the ownership of the files to the **arcsight** user:

```
# chown arcsight:arcsight
/opt/arcsight/connector_esm/current/jre/lib/security/cacerts
```

Proceed to Initializing ArcSight Logger to set up ArcSight Logger.

Initializing ArcSight Logger

ArcSight Logger is pre-installed in ArcSight Express All-in-One. After you have set up the OS and ArcSight ESM through First Boot Wizard, you will initialize Logger by entering basic configurations. Refer to this section for the high-level sequence and specific settings, then refer to the initialization-related topics in the *ArcSight Logger Administrator's Guide* as required.

Logger Initialization Sequence

It is very important that you initialize Logger in the sequence described here. Logger can be reset to its initial condition, but other than that, several of the settings described here cannot be changed after you have set them.

One-time initialization can only be changed by performing a factory reset (see Appendix C, Restoring Factory Settings, on page 71). Be sure you know your required Logger setups before performing the first steps of the initialization sequence (up to rebooting).

1 "Configure Permissions for "arcsight" User" on page 25

2 "Access the Logger User Interface" on page 25

3 "Define Storage Volume" on page 26 – establish where Logger stores event data

4 "Create Storage Groups" on page 26 – apply retention policies to the Storage Volume

5 "Configure Indexing" on page 27 – enable full-text search and select fields

6 "Configure Locale" on page 28 – specify the applicable Locale to display information in the correct formats

7 Reboot the Appliance – reboot to make your storage settings take effect

8 Create SmartMessage Receivers – specify the receiver type

Note

During Logger configuration, you will be reminded to reboot Logger. Ignore these reminders. Postpone rebooting until you have completed the basic Logger configurations.

Configure Permissions for “arcsight” User

By default, ArcSight Logger uses the **oracle** user as the owner of the Logger directory. ArcSight Express All-in-One requires **arcsight** to be the owner. If ownership is not changed, Logger will display an error message at the time you are configuring Storage Volume (see Define Storage Volume). The message will state:

```
Cannot write to /opt/data/logger
```

To change ownership to the logger directory:

As **root**, enter this command:

chown -R arcsight:arcsight /opt/data/logger

This grants the **arcsight** user permission to define storage volume in Logger, as described in Define Storage Volume. After ownership is changed to **arcsight**, Logger no longer displays the error message.

Access the Logger User Interface

Note

During the course of entering Logger initialization settings, Logger will display an alert that reminds you to use Network Time Protocol (NTP) to configure system time manually. You are not required to do this because you have already done so during OS configuration (Step 12 on page 19). You should therefore ignore the reminder and proceed with the initialization process. This alert will go away after you reboot at the end of initialization.

This section describes steps for initial login and for applying the license to Logger. In subsequent Logger logins, you will not be required to re-enter licensing information.

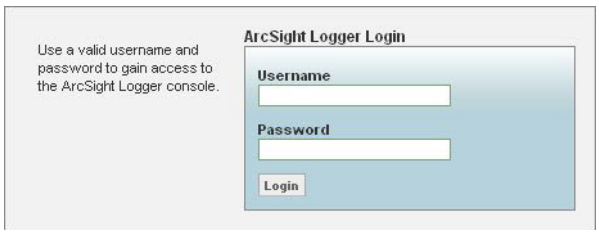
To access the Logger UI on ArcSight Express All-in-One:

1 Use a web browser to access the ArcSight Express All-in-One appliance using its IP address:

https://*<ArcSight Express All-in-One IP address>*

This is the IP address you had configured for ArcSight Express All-in-One during Network Configuration setup beginning on Step b on page 18.

Logger displays the login prompt:



2 Use the default user name (**admin**) and password (**password**) provided with Logger.

3 At the End User License Agreement panel, accept the terms of the EULA and click **Next**.

4 Enter product licensing information and click **Next**.

Both EULA and product licensing information are displayed only at initial login. Subsequent logins to Logger will not display these panels.

5 Proceed to the first step of Logger initiation, Define Storage Volume.

Define Storage Volume

Follow these steps to establish Logger's storage volume.

To define storage volume:

1 Click **Configuration** from Logger's top-level menu bar.

2 Click **Storage** in the left panel.

3 Click the **Storage Volume** tab on the right panel.

Use the following settings for storage volume:

Mount Location	Local
Maximum Size	900
Pre-allocation amount	100% **Note:** Performance is degraded if you don't pre-allocate at least a portion of the storage volume. Allocate 100% as indicated.

Path is not required because your location is local.

4 Click **Save**.

The following sections in the *ArcSight Logger Administrator's Guide* contain more information on storage volumes:

- Chapter 2, *Installation and Initialization*, topic on *3 Storage Volume*
- Chapter 6, *Configuration*, topic on *Storage Volume*

5 Proceed to the next initialization step, Create Storage Groups.

Create Storage Groups

Storage groups are used to support multiple retention policies that fit your requirements. The Default Storage Group has been created for you; you only need to configure its size. You should increase the maximum size of the Default Storage Group and increase the maximum age of the event retention policy to comply with your internal data retention policy.

To configure Default Storage Group:

1 While in **Configuration > Storage**, click the **Storage Groups** tab on the right panel.

2 Click the edit icon corresponding to Default Storage Group.

3 Use the following settings for Default Storage Group (you cannot change the group's name):

Maximum age	90
Maximum size	600

4 Take note of the available space left as displayed by Logger. Based on the maximum size for Default Storage Group, available space left would be **295**.

5 Create another storage group for the remaining available space in the storage volume:

a Click **Add** in the Storage Groups tab in the right panel.

b Enter a name for the new group.

c Specify the maximum age.

d Specify the maximum size based on the remaining available space (**295**).

6 Click **Save**.

The following sections in the *ArcSight Logger Administrator's Guide* contain more information on storage volumes:

- Chapter 2, *Installation and Initialization*, topic on *3 Storage Groups*
- Chapter 6, *Configuration*, topics on *Storage* and *Storage Groups*

7 Proceed to the next initialization step, Configure Indexing.

Configure Indexing

At initialization, Logger prompts you to add a recommended set of fields to the index. The default option on Logger is *No Indexing*. Use indexing options for better performance.

To configure indexing:

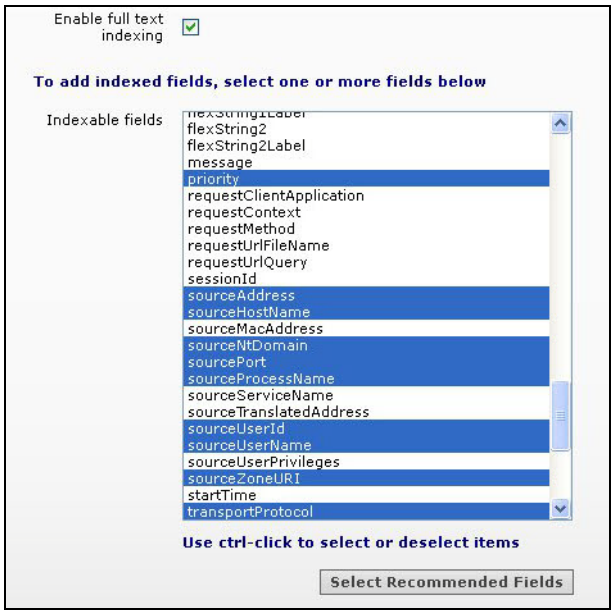
1 Click **Configuration** from the top-level menu bar.

2 Click **Search Optimization** on the left panel.

3 Click the **Search Indexes** tab on the right panel.

4 Click **Enable full text indexing**.

5 Click **Select Recommended Fields** to highlight the set of ArcSight-recommended fields to be added to the index.



6 Click **Apply Changes**.

The following sections in the *ArcSight Logger Administrator's Guide* contain more information on indexing:

- Chapter 2, *Installation and Initialization*, topic on *5 Index Fields and Full-text Indexing*
- Chapter 4, *Searching and Analyzing Events*, topic on *Indexing*

7 Proceed to the next initialization step, Configure Locale.

Configure Locale

The Locale setting ensures that the user interface displays information such as date, time, numbers, and messages in the format and language appropriate for the selected country.

To set the Locale:

1 Click **System Admin** from the top-level menu bar.

2 Click **System Locale** under the System section on the left panel.

3 Choose the country for Locale on the right panel.

4 Click **Save**.

The following sections in the *ArcSight Logger Administrator's Guide* contain more information on locale:

- Chapter 2, *Installation and Initialization*, topic on *5 Locale*
- Chapter 7, *System Admin*, topic on *System Locale*

5 You are now ready to apply your initial settings. Proceed to the next step, "Reboot the Appliance" on page 29.

Reboot the Appliance

At the end of the initialization process, you reboot the appliance using the Logger UI. After the reboot:

- The storage, indexing, and locale settings become permanent.
- Storage volume size can be extended, but not reduced after initialization.
- Only certain settings for non-default storage groups can be changed.
- You can add fields to the index but not remove fields that have been saved.

To reboot:

1. Click **System Admin** from the top-level menu bar.
2. Click **Reboot** on the System section.
3. Click **Start Reboot Now**.

   In about 60 seconds, the appliance reboots. The boot process takes anywhere from 5-10 minutes, during which the system is unavailable.

   The following sections in the *ArcSight Logger Administrator's Guide* contain more information about rebooting Logger:

   - Chapter 2, *Installation and Initialization*, topic on *7 Reboot*
   - Chapter 7, *System Admin*, topic on *Reboot*
4. When the appliance is ready, log back in to Logger ("Access the Logger User Interface" on page 25) and proceed to the next step, "Create SmartMessage Receivers" on page 29.

Create SmartMessage Receivers

Receivers listen for events. Unlike the previous configuration choices for Logger initialization that you cannot change, you can change, disable, enable, and delete receivers as needed. In this procedure, your receiver will be a SmartMessage type.

To create a SmartMessage receiver:

1. Use a web browser to access the Logger UI on the appliance (see "Access the Logger User Interface" on page 25 for information).
2. Click **Configuration** from the top-level menu bar.
3. Click **Event Input/Output** on the left panel, then click the **Receivers** tab on the right panel.
4. Click **Add**.
5. You are presented a series of screens to configure the new receiver. For SmartMessage types, you only need to set the following parameters:

Receiver Name:	Enter a name for the SmartMessage receiver. **Important:** Remember this name because you will be re-entering it in during Forwarding Connector setup.
Receiver Type:	**SmartMessage**
Receiver Encoding:	**UTF-8**

6. Click **Next**.

7 New receivers are initially disabled as indicated by an icon  . Click this icon to enable the new receiver.

The following sections in the *ArcSight Logger Administrator's Guide* contain more information about receivers:

- Chapter 2, *Installation and Initialization*, topic on *8 Receivers* and *SmartMessage*
- Chapter 6, *Configuration*, topic on *Receivers, To Create a Receiver*

After creating the SmartMessage receiver, you will add one or more SmartConnectors and configure them to send messages to Logger. See "Configuring SmartConnectors" on page 32.

You are done with the initial Logger setup in ArcSight Express All-in-One. For the next step, go to Configuring ArcSight Forwarding Connector.

Using a Secondary ArcSight Logger

The Logger component in ArcSight Express All-in-One stores events for up to 90 days. Beyond that period, old events are dropped. You may want to consider installing another Logger appliance as your secondary storage to extend your retention days. The storage appliance comes with its own *Getting Started with ArcSight Logger* document to help you install your newly-purchased storage appliance.

After you have installed the secondary ArcSight Logger, configure the ArcSight Forwarding Connector to send the events to this Logger. 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.

Configuring ArcSight Forwarding Connector

After you have configured Logger, configure ArcSight Forwarding Connector to send events to Logger. ArcSight Forwarding Connector is pre-installed in ArcSight Express All-in-One. The objective of this configuration is to specify ArcSight Manager as the source of events and ArcSight Logger as the destination.

Use this sequence:

- Set Up the Forwarding Connector User in ArcSight Manager–A Forwarding Connector user account is entered in ArcSight Manager, which is the originator of events.
- Set Up Forwarding Connector in ArcSight Express All-in-One–The IP address and receiver name are entered to match the values in the OS and in Logger, respectively.

Set Up the Forwarding Connector User in ArcSight Manager

The first part of the setup instructs you to enter Forwarding Connector information, such as a Forwarding Connector user account, in ArcSight Manager through the Console. You will be performing your setup using multiple ESM resources. This section gives you the steps at a high level. The detailed information is found in the *SmartConnector Configuration Guide for ArcSight Fowarding Connector.*

1 Make sure ArcSight Express All-in-One has been configured properly through First Boot Wizard.

2 Make sure ArcSight Console has been installed. If you have not installed the Console, see "Installing ArcSight Console" on page 37. You will use the Console to enter settings for the Forwarding Connector user.

3 Log in to the Console (default username is **admin** and default password is **password**) and enter ArcSight Express All-in-One's IP address in the Manager field.

4 From the Console's Resource tree on the left, choose **Users**.

5 Right-click a group and choose **New Group**. Give the new group a name, for example, **FwdConnGroup**.

6 Right-click this new group and choose **New User**.

The Inspect/Edit panel for this new user appears to the right of the Console.

7 On the Inspect/Edit's Attributes tab, Login section, use these values and click **Apply**:

User ID	Enter a name, for example, **FwdConn**. This is required.
User Type	Choose **Forwarding Connector**.
Login Enabled	Keep the checkmark.
Password	Enter a password with a minimum of 6 and up to 20 characters. Re-enter to confirm.

8 On the Resource tree on the left, right-click the new group you created in Step 5 and choose **Edit Access Control** from the menu.

The Inspect/Edit panel for this group displays the ACL Editor tab. The Resource field should display Filter.

9 On the ACL Editor tab, click the **Events** tab.

10 Choose the filters to which the Forwarding Connector user has access.

This assumes filters have been defined in the Console. You can edit the user group's access control later to modify the assigned filters.

Set Up Forwarding Connector in ArcSight Express All-in-One

The second part of the setup instructs you to run the Forwarding Connector setup in ArcSight Express All-in-One.

To set up Forwarding Connector:

1 As root, go to this directory:

```
/opt/arcsight/connector_esm/current/bin
```

2 Run this command to launch the connector configuration wizard:

```
./arcsight connectorsetup
```

3 Use the following settings as you go from one screen to the next:

Option	Value
Destination type	Choose **ArcSight Logger SmartMessage**.
Logger Host Name/ IP	Enter the host name or IP address of the ArcSight Express All-in-One appliance. Use the same value you configured during network setup on Step b on page 18.
Receiver Name	Enter the same name you used in "Create SmartMessage Receivers" on page 29.
ArcSight Source Manager Hostname	Enter the host name or IP address of the ArcSight Express All-in-One appliance. Use the same value you configured during network setup on Step b on page 18.
SmartConnector to install	Choose **ArcSight Forwarding Connector (Enhanced)**.
ArcSight Source Manager User Name and Password	Enter the name and password you used for the Forwarding Connector user account in ArcSight Manager. Refer to "Set Up the Forwarding Connector User in ArcSight Manager" on page 30.
SmartConnector Name	Enter a name for the Forwarding Connector. You may use the same name as what you used in ArcSight Console, although you are not required to match it.
SmartConnector Location, Device Location, and Comment	Enter optional information to describe the Forwarding Connector.
Option on how to run the connector	Choose the option to run the connector as a service.

4 When you are finished, restart the Forwarding Connector with the following command:

```
/etc/init.d/arc_esm_connector restart
```

The restart enables your settings to take effect.

Refer to the topic on sending events to ArcSight Logger in the *SmartConnector Configuration Guide for ArcSight Forwarding Connector* for details.

Configuring SmartConnectors

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.

On ArcSight Express All-in-One's Logger, you are provided two containers. You have the option to add a total of eight SmartConnectors locally (four per container). As seen on the Logger UI, the containers belong to the host called Localhost, and Localhost belongs to the location called Default.

To view the containers and add connectors:

1. Use a web browser to access the Logger UI on the appliance (see "Access the Logger User Interface" on page 25 for information).
2. Click **Configuration** on the top-level menu bar.
3. Click **Manage Connectors** and click **System** on the left panel.
4. Expand **Default**, then expand **Localhost** on the left panel.

   Container 1 and Container 2 are displayed. You can add your SmartConnectors to these containers.
5. Choose the container to which you want to add the SmartConnector. Under the Action column, click the icon for adding a connector.
6. Choose the connector from the pull-down list of available types, then click **Next**.

For specific information on a SmartConnector, refer to that SmartConnector's configuration guide.

7. Enter basic parameters specific to the connector type. Make sure to use the following settings to enable this connector to send events to Logger:

IP address:	Use the ArcSight Express All-in-One IP address.
Port	**443**
Receiver name	Enter the same name you used in "Create SmartMessage Receivers" on page 29. **Note**: If you decide to change the receiver name later, remember you must change it consistently in three places: Logger configuration for SmartMessage receiver, Forwarding Connector for receiver name, and the Logger SmartConnector parameter for receiver name.

8. For primary destination, specify **ArcSight Logger SmartMessage**.
9. Enter additional details about the connector such as a descriptive name, the location (for example, use the ArcSight Express All-in-One hostname), and other additional comments.
10. Click **Done**.

The following section in the *ArcSight Logger Administrator's Guide* contains more information about connectors:

Chapter 8, *Managing Connectors*

Configuring ArcSight TRM (Threat Response Management)

If you want to use ArcSight TRM, follow the instructions in Chapter 4, Using ArcSight TRM™ in ArcSight Express All-in-One, on page 47 to configure the TRM service.

Important: If you are *not* using ArcSight TRM at this time, run the following commands as **root**:

```
sp=`/sbin/service trm status postgresql`
sd=`/sbin/service trm status daemontools`
if [[ $sp == DOWN* && $sd == UP* ]];
then
  /sbin/service trm stop daemontools;
fi
```

Run the commands only once.

The reason for the above solution is because certain TRM processes are automatically running and they generate messages that may fill up the logs. The above commands will prevent problems with the logs filling up. Subsequent reboots of the ArcSight Express All-in-One appliance will not require you to re-run the commands. If you decide to use ArcSight TRM in ArcSight Express All-in-One later, then follow the procedures in Chapter 4, Using ArcSight TRM™ in ArcSight Express All-in-One, on page 47.

Installing ArcSight IdentityView Express and Active Directory Model Import Connector

If you want to use IdentityView, you need to manually install and configure it using ArcSight Console. The installation files and related documents are in the following directory in ArcSight Express All-in-One:

```
/root/IdentityViewExpress.installers
```

This directory includes the necessary files for IdentityView Express and the Active Directory Model Import Connector.

To install IdentityView:

1. If ArcSight Console is not yet installed, follow the instructions in Chapter 3, Installing ArcSight Console, on page 37. Note that the Console should be installed in a separate system, *not* in ArcSight Express All-in-One.
2. From the ArcSight Express All-in-One appliance, copy the ARB file:

```
/root/IdentityViewExpress.installers/ArcSight-SolutionPackage-IdentityViewExpress.1.1.1.6460.arb
```

   to the system where you had installed the Console.

3. Consult the *ArcSight Deployment Guide for IdentityView Express* for procedures to upload the ARB file through the Console. The procedures are included in the section on installing the IdentityView package.
4. On the ArcSight Express All-in-One appliance, add the Active Directory Model Import Connector as follows:
   a. Open a command shell and log in as **root**.
   b. Enter the following command:

```
chmod +x
/root/IdentityViewExpress.installers/ArcSight-4.7.6.5515.0-ADIdentityModelConnector-Linux.bin
```

   This converts the connector file to an executable.

c Install the Active Directory Model Import Connector according to the instructions found in *SmartConnector Configuration Guide for Microsoft Active Directory Identity Model*.

Updating ArcSight Express

After configuration, the ArcSight Express All-in-One appliance model V7400 is at ArcSight Express v5.0 SP1 Patch 1. If you have this appliance, make sure to upgrade the ArcSight Express component to v5.0 SP1 Patch 2.

Refer to the *ArcSight Express Upgrade Guide, ArcSight All-in-One 2.0*, for the instructions.

Next Steps

You are now ready to configuring additional software components if you want to take advantage of their features. These include:

- ArcSight TRM

  See Chapter 4, Using ArcSight TRM™ in ArcSight Express All-in-One, on page 47.

- ArcSight IdentityView Express

  See the following documents:

  - *ArcSight Deployment Guide, IdentityView Express*
  - *ArcSight Solution Guide, IdentityView*
  - *ArcSight IdentityView Express Release Notes*
  - *ArcSight SmartConnector Configuration Guide for Microsoft Active Directory Actor Model*
  - *Release Notes, SmartConnector for Microsoft Active Directory Actor Model*

Chapter 3

Installing ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks on ArcSight Express All-in-One™ appliance, 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 All-in-One appliance. This chapter explains how to install and configure the ArcSight Console.

Make sure that you have successfully configured the ArcSight Express All-in-One appliance before proceeding.

The following topics are covered in this chapter:

ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight All-in-one appliance.

Console Supported Platforms

The ArcSight Console is supported on the following operating systems.

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 XP Professional SP3 32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM

Using a PKCS#11 Token

ArcSight supports the use of a PKCS#11 token, such as the Common Access Card (CAC), which is used for identity verification and access control. PKCS#11 is a public key cryptography standard which defines an API to cryptographic tokens.

Installing the Console

Do not install the ArcSight Console on the ArcSight Express All-in-One appliance. See the section "Console Supported Platforms" on page 37 for supported platforms for ArcSight Console.

On Macintosh platforms, please make sure that:

- You are using an intel processor based system
- You have JRE 1.6 installed on your system before installing the Console.
- If you are installing the Console on a new system for the first time, or if you have upgraded your system causing the JRE update, your Console installation might fail. To work around this issue, make sure that you change the permissions on the cacerts file to give it write permission before you import it.

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.

On Macintosh platform, if your JRE gets updated, you will see the following error when you try to log into the Console:

```
IOException: Keystore was tampered with or password was incorrect.
```

This happens because the Mac OS update changed the password for the cacerts file in the system's JRE. To work to around this issue, before you start the Console, change the default password for the `cacerts` file by setting it to the following in the `client.properties` file (create the file if it does not exist) in the Console's `/current/config` folder by adding:

```
ssl.truststore.password=changeme
```

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.

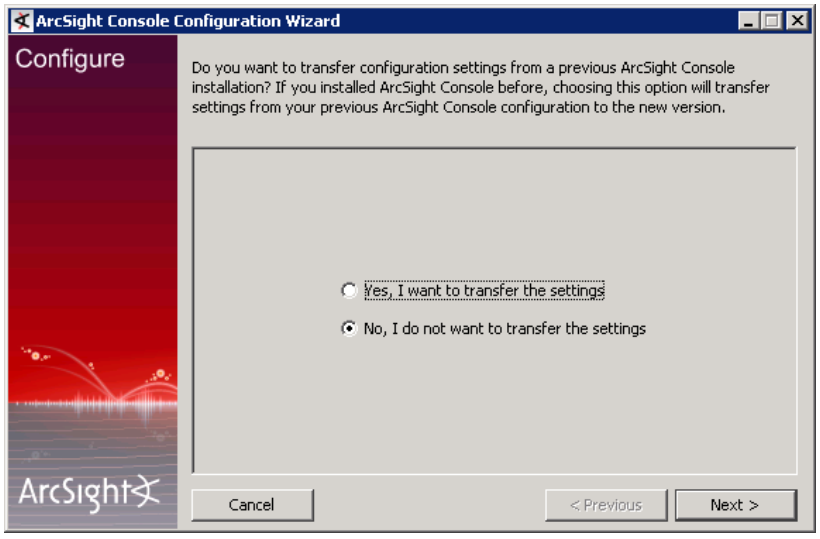
Platform	Installation File
Linux	ArcSight-5.0.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-5.0.x.nnnn.y-Console-Win.exe

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.

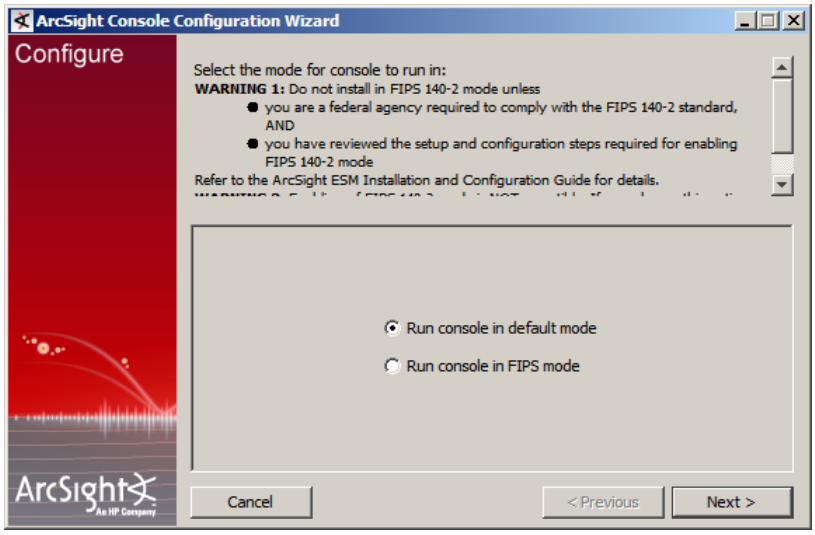


Selecting the Mode in which to Configure ArcSight Console

Note

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

Next, you will see the following screen:



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

Manager Connection

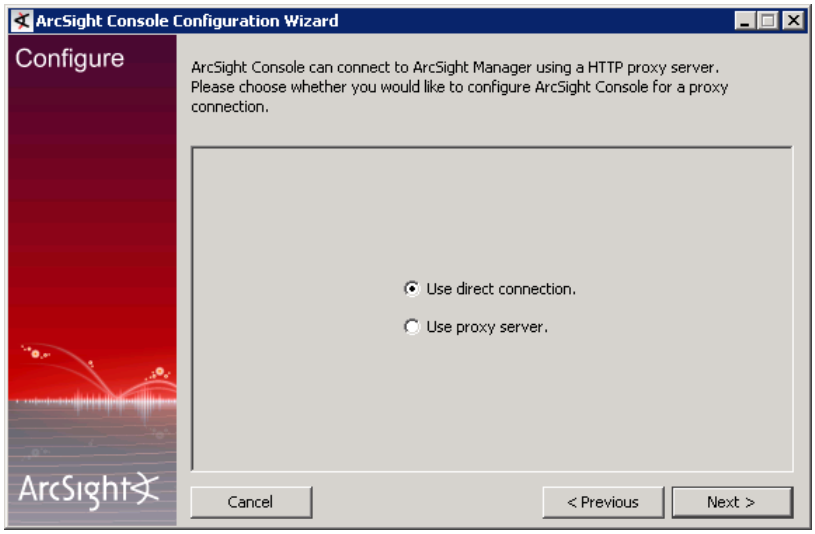
The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. The hostname is the ArcSight Express All-in-One Appliance host name or its IP address. The Manager host name that you had entered in the First Boot Wizard while configuring the ArcSight Express All-in-One 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.

Caution

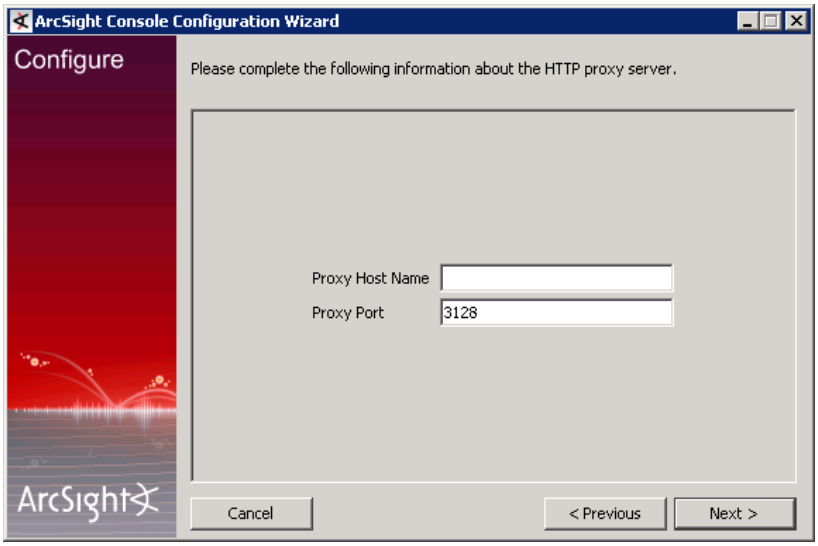
Do not change the Manager's port number.

Click **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.



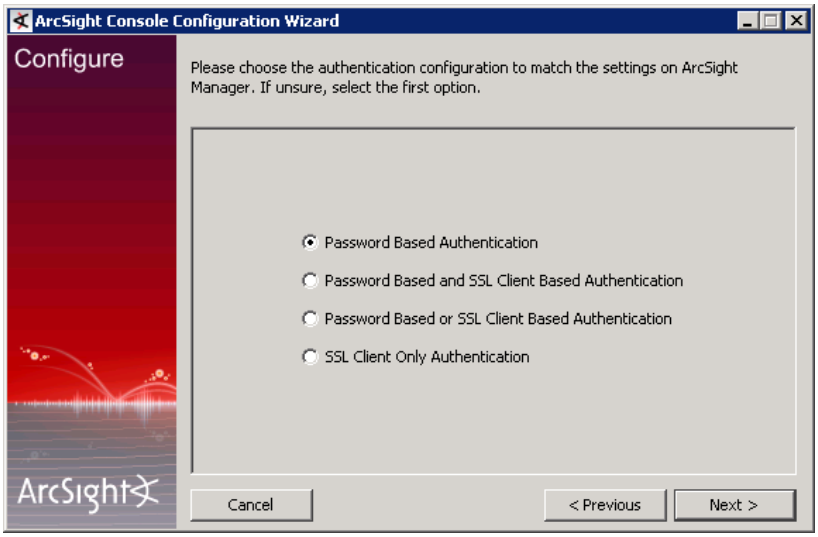
If you select the Use proxy server option, you will be prompted to enter the proxy server information.



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:



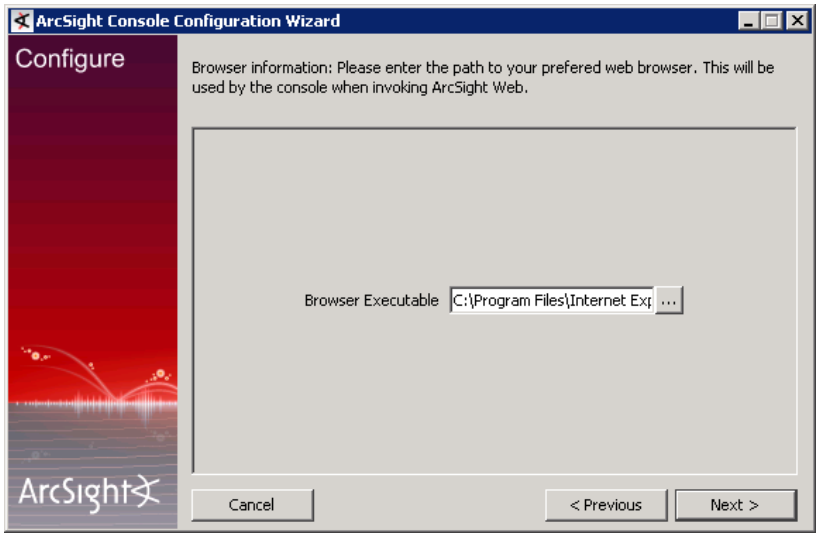
This release of ArcSight Express All-in-One appliance supports **Password Based Authentication** only.

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

Web Browser

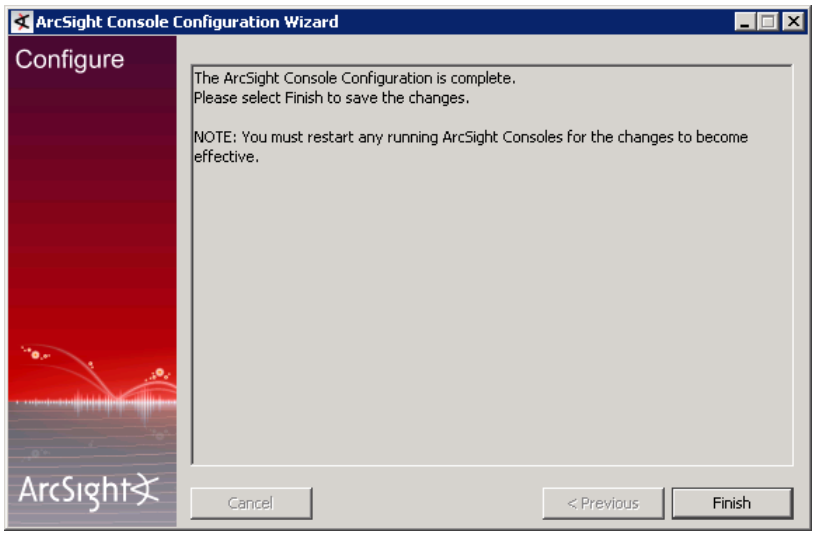
The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Base articles, and other web page content.

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**.



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

The Manager on ArcSight Express All-in-One 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.

If you just finished installing Console for the ArcSight Express All-in-One appliance model V7400, note that the Console is at version 5.0 SP1 Patch 1. You need to upgrade Console to 5.0 SP1 Patch 2. Refer to the *ArcSight Express Upgrade Guide, ArcSight Express All-in-One v2.0* for instructions on how to upgrade your Console.

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
```

To uninstall on Unix hosts, open a command window on the `<ARCSIGHT_HOME>/UninstallerData` directory and run the command:

```
./Uninstall_ArcSight_Console
```

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

Chapter 4

Using ArcSight TRM™ in ArcSight Express All-in-One

This chapter is written for users who want to take advantage of ArcSight TRM™ (Threat Response Manager) functionality that is available with ArcSight Express All-in-One.

This chapter covers the following topics:

Details about ArcSight TRM are documented in the *ArcSight NSP Installation and Configuration Guide*. You will be referred to specific topics in that guide from time to time. Keep in mind, however, that the guide is oriented towards NSP (and TRM) being in a separate appliance; therefore, not all topics apply to ArcSight Express All-in-One. When configuring software components, therefore, you should consistently use the appliance's IP address and host name in all software components.

Adding and Starting the TRM Service

The following commands help you add and start the TRM service. These are the prerequisite steps before configuring ArcSight TRM in ArcSight Express All-in-One.

As **root**, enter the following commands:

```
service trm add

service trm start
```

Configuring ArcSight TRM

This topic describes procedures to configure ArcSight TRM in ArcSight Express All-in-One, which you will perform in the following sequence:

1. Enter Network Settings using the NSP interface.
2. Add the ArcSight TRM SmartConnector using the Logger interface.
3. Define ESM Rules using ArcSight Console.

Enter Network Settings

You need to enter the IP address and gateway that match the settings entered during OS configuration. You will do this in the NSP interface (TRM is one of the function tabs of the NSP interface).

As directed in the following procedure, use the same network settings in TRM as those in your OS. If they don't match, the next time you reboot the ArcSight Express All-in-One appliance, TRM network settings will overwrite the appliance's OS network settings. As a result, the appliance will not start up successfully. Follow the procedures exactly as shown.

To enter network settings:

1 Access the NSP interface by entering the following URL in your browser:

https://*<ArcSight Express All-in-One IP address>*:1443

This is the IP address you had configured for ArcSight Express All-in-One during setup beginning on Step b on page 18. The port number is for TRM use.

2 Log in to the NSP interface using the default administrator username and password:

- Username: **admin**
- Password: **temp1234**

Make sure to change the admin password later. For more details, refer to the User Administration chapter of the *NSP Installation and Administration Guide*.

3 Click the **Admin** tab >**System** > **Settings**.

4 Use the following settings:

- For Default Gateway, enter the address of your production environment's gateway.
- For **Eth0**, make sure it matches the address you entered during OS setup at Step b on page 18.
- For **Hostname**, use the hostname you entered during OS setup at Step a on page 19.
- For Allow System Ping, click **Yes**.
- To save changes, click **Update Settings**.

5 Verify that the information in the other System Setting tabs (for example, DNS, SMTP, Static Routes, and so forth) are the correct settings used by the ArcSight Express All-in-One appliance.

For more information about TRM and its settings, refer to the Threat Response Manager chapter of the *ArcSight NSP Installation and Administration Guide*.

Add the ArcSight TRM SmartConnector

ArcSight TRM uses the Threat Response Manager (TRM) SmartConnector to integrate with ArcSight ESM. In the following procedures, you will use the Logger interface to add the TRM SmartConnector.

Related documentation

ArcSight Logger Administrator's Guide

SmartConnector Configuration Guide for ArcSight Threat Response Manager

Installation and Administration Guide, ArcSight NSP

- Chapter 6 has more details about Threat Response Manager.
- Chapter 10 has more details on TRM and Arcsight ESM integration.

Note that the ArcSight NSP guide assumes that TRM is in the Network Synergy Platform (NSP) appliance. Keep in mind that in this case, TRM is in ArcSight Express All-in-One.

To add Threat Response Manager SmartConnector to Container 1

1. Access the Logger interface by entering the following URL in your browser:

   https://<*ArcSight Express All-in-One IP address*>

2. Log in to Logger. The default login name is **admin** and the default password is **password**.
3. Click **Configuration** on the top-level menu bar.
4. Click **Manage Connectors** and click **System** on the left panel.
5. Expand **Default**, then expand **Localhost** on the left panel.
6. Click **Container 1** and add the SmartConnector as follows:
   a. Under the Action column, click the icon for adding a connector.
   b. Choose **ArcSight Threat Response Manager connector** from the pull-down list and click **Next**.
   c. Enter basic parameters for this connector. For Destination, use ***<ArcSight Express All-in-One IP address>*:1443**, which is TRM's port number.
   d. For Primary Destination, specify **CEF Syslog**.
   e. Enter additional details about the connector such as a descriptive name (for example, use the ArcSight Express All-in-One hostname), the location, and other additional comments.
7. Click **Done**.

Adding TRM SmartConnector to Container 2

For the purposes of ArcSight Express All-in-One, Arcsight recommends that you add the TRM SmartConnector to Container 1. However, if you have already reached the maximum limit for Container 1 (four) and you need to add another TRM SmartConnector, you may add it to Container 2.

1. Follow the same basic instructions in To add Threat Response Manager SmartConnector to Container 1.
2. As **root**, use the following command to create the `endorsed` directory:

```
mkdir -p /opt/arcsight/connector_2/current/jre/lib/endorsed/
```

3 Copy the `saaj.jar` file, which is required by TRM, to the `endorsed` directory :

```
cp -pv /opt/arcsight/trm/local/tomcat/webapps/nwsapi/WEB-INF/lib/saaj.jar \
/opt/arcsight/connector_2/current/jre/lib/endorsed/saaj.jar
```

4 Restart the connector:

```
/sbin/service  arc_appliance_connector_2 restart
```

Define ESM Rules

Related documentation

ArcSight ESM Console User's Guide, chapter on *Rules*

After you have added and configured the TRM SmartConnector, you are ready to define ESM rules that trigger TRM actions. You will need ArcSight Console for rule definition tasks. If you have not yet installed the Console, refer to "Installing ArcSight Console" on page 37. You should install the Console in a separate system and *not* in ArcSight Express All-in-One.

As an option, you can run TRM commands through ArcSight Console. Refer to the *ArcSight ESM Console User's Guide*, chapter on *Integration Commands*.

Restoring TRM Data from Backups

Assuming you have created a backup of your TRM data, you can follow the instructions here to restore the backup. For procedures to create a backup, see Chapter 3, *Configuring the NSP Appliance*, topic on *Backing Up and Restoring Data* in the *ArcSight NSP Installation and Administration Guide*.

To restore TRM data from backups in the ArcSight Express All-in-One appliance, perform the steps on the NSP user interface. Then continue the restoration process with shell commands.

To restore TRM data from backups:

1 Access the NSP interface by entering the following URL in your browser:

https://*<ArcSight Express All-in-One IP address>*:1443

2 Log in to the NSP interface as a user with admin privileges.

3 Click **Admin > System > Backup & Restore**.

4 On the Backup Up & Restore page, click **Restore From Backup**.

5 Browse to and select your previously-created backup file or enter the filename, then click **Upload Backup** to upload.

A message states that the backup is uploaded and verified.

Do *not* click **Verify and Begin Restore** button. Restoring the backup in this manner will not work and will cause system problems.

6 Close the browser window or navigate to another TRM page to avoid problems with the Verify and Begin Restore button.

7 As **root**, enter the following shell commands to restore the TRM backup file and restart the TRM service:

```
service trm stop
service trm start postgresql
file=`find /opt/backups/restore/*/opt/backups/ \
  -type f -not -name '*.md5' \
  -printf "%CY%Cm%Cd-%CT %p\n" \
  | sort | cut -d' ' -f2 | tail -1`
echo "Restoring database from backup using file: $file"
/opt/arcsight/trm/local/pgsql/bin/dropdb \
  --port 11976 --username cprpgsql rwdb
cat $file | /opt/arcsight/trm/local/pgsql/bin/psql \
  --port 11976 --username cprpgsql -d template1
service trm start
exit
```

8 Verify the network settings that you have restored from backup, making sure they match the settings of the ArcSight Express All-in-One operating system. On the NSP UI, under System, select **Settings > Admin > Network** and verify the following.

- Make sure **Eth0** matches the address you entered during OS setup at Step b on page 18.
- Make sure **Hostname** matches the hostname you entered during OS setup at Step a on page 19.

The network settings in TRM must match those in your OS. If they don't match, the next time you reboot the appliance, TRM network settings will overwrite the OS network settings. As a result, the appliance will not start up successfully.

9 Verify that the information in the other System Setting tabs (for example, DNS, SMTP, Static Routes, and so forth) are correct. These will be used by the appliance.

TRM Commands

This topic describes some useful commands to use the TRM service in ArcSight Express All-in-One.

For more information about TRM functionality, refer to the TRM chapter of the *ArcSight NSP Installation and Administration Guide*.

To use TRM, run the following commands in a root shell:

Command	Description
/sbin/service trm add	Configure TRM to use the same license as other applications, and configure the system to start or stop TRM processes during bootup or shutdown. Print a running summary of status. After this command succeeds, any reboot will restart TRM, so a user might only need to manually add and start TRM one time.

Command	Description
/sbin/service trm start	Start all TRM processes running. Print a summary of TRM startup status. TRM startup typically completes in a few seconds.
/sbin/service trm stop	Stop all TRM processes that are running. Display a summary of TRM shutdown status. TRM shutdown typically completes in a few seconds.
/sbin/service trm help	Provide information on TRM service actions such as **list**, **restart**, **status**, and **stop**.

Appendix A

Troubleshooting

The following information may help solve problems that might occur during installation, setup, and use of ArcSight Express All-in-One. In some cases, the solution can be found here or in other documentation, but ArcSight Customer Support is available if you need it. This chapter covers the following topics:

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 locations:

Component	Location
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_esm/current/logs
ArcSight Logger	/opt/arcsight/logger/logs
Container 1 for SmartConnectors	/opt/arcsight/connector_1/current/logs
Container 2 for SmartConnectors	/opt/arcsight/connector_2/current/logs
ArcSight Logger onboard connector	/opt/arcsight/connector/current/logs
ArcSight TRM	/opt/arcsight/trm/local/apache/logs/access_log* /opt/arcsight/trm/local/apache/logs/error_log* /opt/arcsight/trm/local/pgsql/data/serverlog* /opt/arcsight/trm/local/tomcat/logs/* /var/log/messages /var/log/secure /var/log/dmesg /opt/updates/*.log /opt/arcsight/trm/ENIRA/data/temp/* /opt/arcsight/trm/ENIRA/data/debug/* /opt/arcsight/trm/ENIRA/data/insp_log* /opt/arcsight/trm/ENIRA/data/exceptions.log*
ArcSight Console	<ARCSIGHT_HOME>\current\logs **Note**: Console is not installed in the ArcSight Express All-in-One appliance.

Starting or Stopping Services

This section provides a reference of commands for manually starting and stopping services.

Services in the ArcSight Express All-in-One appliance are configured to start automatically after the appliance is rebooted. For ArcSight TRM commands, refer to "Using ArcSight TRM™ in ArcSight Express All-in-One" on page 47.

To stop or start ArcSight Manager

1. Log in as **root** and go to the /etc/init.d directory.
2. To start ArcSight Manager, use

```
./arcsight_manager start
```

To stop ArcSight Manager, use

```
./arcsight_manager stop
```

To stop or start ArcSight Web

1. Log in as **root** and go to the `/etc/init.d` directory.
2. To start ArcSight Web, use

   ```
   ./arcsight_web start
   ```

   To stop ArcSight Web, use

   ```
   ./arcsight_web stop
   ```

To stop or start Forwarding Connector

1. Log in as **root** and go to the `/etc/init.d` directory.
2. To start Forwarding Connector, use

   ```
   ./arc_esm_connector start
   ```

   To stop Forwarding Connector, use

   ```
   ./arc_esm_connector stop
   ```

To stop or start ArcSight Logger

1. Log in as **root**.
2. To stop ArcSight Logger, use

   ```
   /opt/local/monit/bin/monit stop all
   ```

   To start ArcSight Logger, reboot the appliance.

Customizing ESM Components Further

First Boot Wizard configures the software components on ArcSight Express All-in-One (ArcSight Database, ArcSight Manager, and ArcSight Web) 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 **oracle**, run the following command from `/opt/arcsight/db/bin`:

```
./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`:

```
./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 Download Center.

ArcSight Forwarding Connector

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

```
./arcsight connectorsetup
```

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

Replacing the License

You may need to replace your ArcSight Express All-in-One license (`arcsight.lic`) when it expires or you are moving from a demo to a user license. Contact ArcSight Customer support for the required license. Follow these instructions:

1. As **root**, run the following commands:

   ```
   cd /opt/arcsight/manager/bin
   ```

   ```
   ./arcsight deploylicense
   ```

   This launches the License Deployer Wizard.
2. Follow the steps in the wizard to upload the new license file.
3. Reboot the appliance to apply the new license.

Fatal Error When Running First Boot Wizard

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

To resolve this issue, try the following steps:

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

> **Note** To run the commands at this step, you must be logged in as the Oracle user. If you are not the Oracle user, first run the command to switch user:
>
> ```
> # su - oracle
> ```

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

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

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

```
% ./arcdbutil sql

Enter user-name: / as sysdba
```

You will get the `sqlplus` prompt only if the Oracle services are running.

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

```
./arcsight appliancefirstbootsetup
```

First Boot Wizard can only be re-run 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 ArcSight Express All-in-One to its factory settings. For instructions on how to do this, see Appendix C, Restoring Factory Settings, on page 71.

Manager Service Fails When Starting

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

1 Start the Manager service manually. See Step 3 on page 58 for information on how to start the Manager service manually.

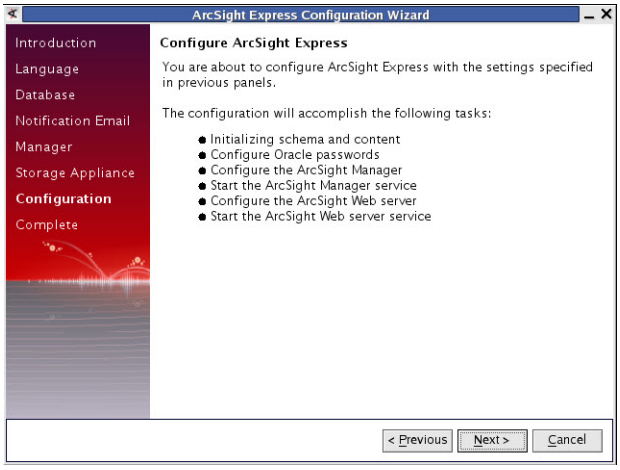
2 Configure the Forwarding Connector and ArcSight Web manually. See “Failed” Status While Configuring or Starting a Component section for details on how to run Forwarding Connector and ArcSight Web setups manually.

3 Run the tablespace expansion manually. See Step 2 on page 58 for details on how to do this.

In the event that any of the above steps do not work, we recommend that you revert ArcSight Express All-in-One to its factory settings. For instructions on how to do this, see Appendix C, Restoring Factory Settings, on page 71.

“Failed” Status While Configuring or Starting a Component

If you cancel out of First Boot Wizard before you reach the screen below, you can re-run the wizard.



However, if you click Next in the screen above and the configuration begins, and if any step fails or you cancel out of the wizard, you will be required to run the corresponding component setup program and configure the component manually.

If you see a “Failed” status for any component, such as the following, you must 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 54 for the location of the logs.

To configure components 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` on ArcSight Express All-in-One 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 Download Center.

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

   ```
   ./arcsight database xts
   ```

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

```
./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 `/opt/arcsight/connector_esm/current/bin` on ArcSight Express All-in-One 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 Download Center download site.

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

```
./arcsight_web start
```

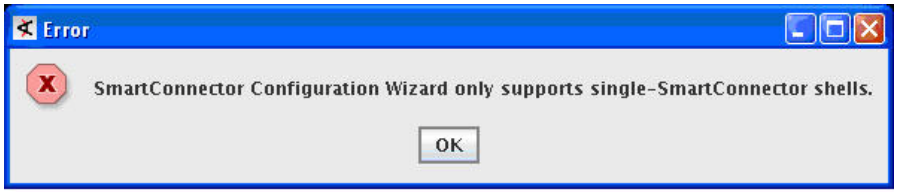
7 To manually start a Forwarding Connector service, run the following command from `/etc/init.d` on ArcSight Express All-in-One as **root**:

```
./arc_esm_connector start
```

In the event that any of the above steps do not work, we recommend that you revert ArcSight Express All-in-One to its factory settings. For instructions on how to do this, see Appendix C, Restoring Factory Settings, on page 71.

Error When Running SmartConnector Setup Wizard

If you are starting the SmartConnector setup wizard, you may encounter this error:



This is because the wizard is used only for single-SmartConnector setup. Most likely, you have multiple SmartConnectors in the same container.

If you get this error, use the Logger UI's **Configuration > Manage Connectors** interface to edit SmartConnectors.

Changing Network Settings After Configuring Them in First Boot Wizard

ArcSight Express All-in-One is identified in the network either by IP address or by host name. This was set when you boot the ArcSight Express All-in-One appliance for the first

time and configured the OS using First Boot Wizard. After First Boot Wizard has run successfully, you will not be allowed to run the wizard again.

In case you want to change the IP address or host name of the appliance after you have successfully completed configuration through First Boot Wizard, refer to one of the following topics:

- "Changing the IP Address After Configuring It in First Boot Wizard" on page 60
- "Changing the Host Name After Configuring It in First Boot Wizard" on page 62

Changing the IP Address After Configuring It in First Boot Wizard

Some reminders:

- Run Manager and Web setup commands as **arcsight**.
- Run all other commands as **root**.
- Start and stop all services as **root**.

In case you want to change the IP address of the appliance after running 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` as **root**:

      ```
      ./arcsight_manager stop
      ```

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

      ```
      ./arcsight_web stop
      ```

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

      ```
      /opt/local/monit/bin/monit stop connector_esm
      ```

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

   ```
   ./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. If you are running TRM, enter the new IP address in TRM. See "Enter Network Settings" on page 48.
6. Reboot the ArcSight Express All-in-One appliance.

   If you had entered an IP address when prompted for a Manager Host Name in First Boot Wizard, then you will be required to do the following additional steps:

7 As **root**, stop the Manager and Web services again. These services would have started upon reboot.

8 Run the following to start the setup program for the Manager from `/opt/arcsight/manager/bin`:

```
./arcsight managersetup
```

This will open the Manager's setup wizard.

a Enter the new IP address that you set for your appliance in Step 4 above 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 IP address.

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

```
./arcsight_manager start
```

10 Import the Manager's newly generated self-signed certificate on the webserver using the `keytoolgui` tool. See the *ArcSight ESM Administrator's Guide* available on the ArcSight Download Center for details on how to do this.

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

```
./arcsight websetup
```

a Enter the new IP address in Webserver Host Name field when prompted.

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 IP address.

12 If you chose to set up Logger and Forwarding Connector when configuring ArcSight Express All-in-One using the First Boot Wizard, stop the Forwarding Connector service by running the following command as **root**:

```
/opt/local/monit/bin/monit stop connector_esm
```

13 Import the Manager's certificate on the connector using `keytoolgui`. See the *ArcSight ESM Administrator's Guide* available on the ArcSight Download Center for details on how to do this.

14 Run the setup program for the connector from `/opt/arcsight/connector_esm/current/bin`:

```
./arcsight connectorsetup
```

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

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

```
./arc_esm_connector start
```

16 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 Download Center for details on how to do this.

17 Test to make sure that the clients can connect to the Manager.

Changing the Host Name After Configuring It in First Boot Wizard

Some reminders:

- Run Manager and Web setup commands as **arcsight**.
- Run all other commands as **root**.
- Start and stop all services as **root**.

In case you want to change the host name of ArcSight Express All-in-One after running 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` as **root**:

   ```
   ./arcsight_manager stop
   ```

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

   ```
   ./arcsight_web stop
   ```

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

   ```
   ./arc_logger_connector stop
   ```

2 Stop the TNS Listener by running the following command from `/opt/arcsight/db/bin`:

   ```
   ./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 ArcSight Express All-in-One.

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`:

```
arcdbutil listener start
```

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

```
./arcsight database pc
```

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

12 If you are running TRM, enter the new host name in TRM. See "Enter Network Settings" on page 48.

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

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

```
./arcsight_manager start
```

14 Start the Web by running the following command from `/etc/init.d` 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:

15 Stop the Manager.

16 Run the Manager's setup program from `/opt/arcsight/manager/bin` 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.

17 Start the Manager service by running the following command from `/etc/init.d` as user **root**:

```
./arcsight_manager start
```

18 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 Download Center for details on how to do this.

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

```
./arcsight websetup
```

20 Enter the new host name in the Manager Host Name and the Webserver Host Name fields when prompted.

21 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 `/etc/init.d` as **root**:

```
/opt/local/monit/bin/monit stop connector_esm
```

22 Import the Manager's certificate on the connector using `keytoolgui`. See *ArcSight ESM Administrator's Guide* available on the ArcSight Download Center for details on how to do this.

23 While logged in as **root**, run the setup program for the connector from `/opt/arcsight/connector_esm/bin`:

```
./arcsight connectorsetup
```

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

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

```
./arc_esm_connector start
```

25 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 Download Center for details on how to do this.

26 Test to make sure that the clients can connect to the Manager.

Appendix B

Default Settings for Components

This appendix gives you the default settings for each software component in ArcSight Express All-in-One. It covers the default settings for the following:

You can always customize any component by running its setup program. Refer to Appendix A, Troubleshooting, on page 53 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

ArcSight Express All-in-One comes pre-installed with Oracle 11g Release 2. 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
Number of data files	16 data files and 32 index files
Data file 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	96 GB (6 files x 12 GB)
ARC_EVENT_INDEX	192 GB (12 files x 16 GB)
ARC_UNDO	64 GB (8 files x 8 GB)
ARC_TEMP	32 GB (4 files x 8 GB)
Language in which default system content resources will be installed	English
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/arcsight
Database Host name	Host name or IP address of your ArcSight Express All-in-One appliance
Database port number	1521
Database instance name	arcsight

Setting	Default Value
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	Large
Database Character set	UTF-8
Allowed TNS Clients	localhost
Auto Archive Redo logs	No
Initialize Tablespaces, Schema, and Resources	Yes
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 All-in-One

ArcSight Express All-in-One 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 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 ArcSight Console™ and through 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 All-in-One allows, forward the events to ArcSight Logger.

ArcSight Manager™

ArcSight Manager uses a self-signed certificate, which is 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	`/opt/arcsight/manager`
Manager host name	Host name or IP address of the ArcSight Express All-in-One appliance
Manager Port	`8443`
Manager license file	Obtain from ArcSight Customer Support
Packages installed	ArcSight Express, ArcSight Administration
Java Heap Memory	2048 MB
Authentication Type	Password-based
Type of certificate used	Self-signed
Default password for keystore	`password`
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 for you:

Setting	Default Value
Location of ArcSight Web	`/opt/arcsight/web`
ArcSight Web host name	Host name or IP address of the ArcSight Express All-in-One appliance

Setting	Default Value
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 Logger 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_esm
ArcSight Forwarding Connector installed as service	Yes
Name of the Forwarding Connector Service	arc_logger_connector

ArcSight Logger

The ArcSight Express All-in-One includes the ArcSight Logger for connector management with two containers.

Setting	Default Value
Location of ArcSight Logger	/opt/arcsight/logger
ArcSight Logger host name	IP address of the ArcSight Express All-in-One appliance
ArcSight Logger Port	443
Maximum Logger storage volume	900 GB
Container 1 for SmartConnectors	/opt/arcsight/connector_1
Container 2 for SmartConnectors	/opt/arcsight/connector_2

Appendix C

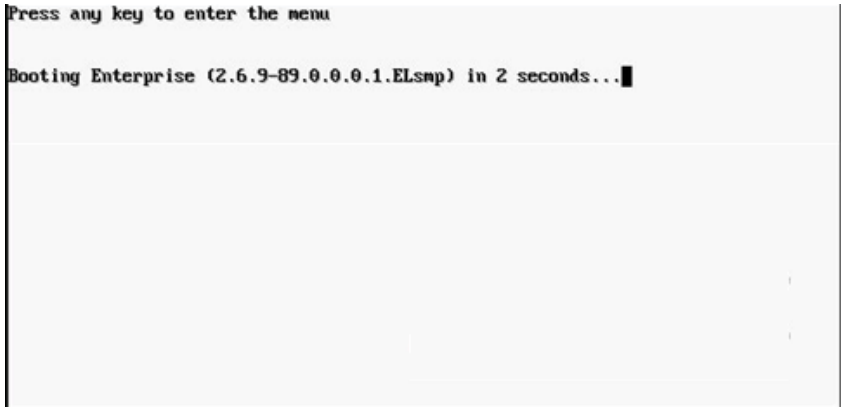
Restoring Factory Settings

You can restore ArcSight Express All-in-One to its original factory settings using the built-in Acronis True Image software.

Restoring ArcSight Express All-in-One to factory settings will irrevocably delete all event data and configuration settings.

To restore ArcSight Express All-in-One to its original factory settings, perform these steps:

1. Attach a keyboard, monitor, and mouse directly to the appliance.
2. Reboot ArcSight Express All-in-One.



3. At the next screen, use the mouse or arrow key on your keyboard to select **System Restore** and press Enter.
4. Click **Acronis True Image Server** to continue.
5. In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press Enter.
6. When the Restore Data Wizard starts, click **Next** to continue.
7. On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.
8. On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.
9. On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** and click **Next**.

10 On the **NT Signature selection for image restoration** page, select **Generate new NT signature** and click **Next**.

11 On the **Restored Hard disk Location** page, select the **cciss/c0d0** drive to restore and click **Next**.

12 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**.

13 On the **Next Selection** page, select **No, I do not** and click **Next** (there are no other partitions or disks to restore).

14 Validating the archive before restoring is optional. On the **Restoration Options** page:

a Select **Validate backup archive before restoration** 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**.

15 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 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.

16 When you see a message indicating that the data was restored successfully, click **OK**.

17 If you specified automatic reboot in Step 14, the appliance reboots when the restore is complete. Otherwise, reboot the appliance manually.

Index