Configuration Guide

ArcSight Express™ v3.0
Featuring ESM with CORR-Engine

August 2011

ArcSight™
An HP Company

Configuration Guide ArcSight Express™ v3.0

Revision History

Date	Product Version	Description
08/01/11	ArcSight Express™ v3.0	New Document

ArcSight Customer Support

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

Contents

Chapter 1

What is ArcSight Express v3.0?

ArcSight Express v3.0 introduces the Correlation Optimized Retention and Retrieval Engine Storage (CORR-Engine Storage), a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches. This provides a number of benefits, including increased performance and more compact data storage.

This chapter covers the following topics:

Pre-installed Components on ArcSight Express v3.0

The ArcSight Express v3.0 Appliance has the following software components pre-installed on it:

- ArcSight Manager
- ArcSight CORR-Engine (Correlation Optimized Retention and Retrieval Engine)

ArcSight Manager

ArcSight Manager is at the center of the ArcSight Express v3.0 Appliance. The Manager is a software component that functions as a server that receives event data from Connectors and correlates and stores them in the database. The Manager also provides advanced correlation and reporting capabilities.

ArcSight CORR-Engine

ArcSight CORR-Engine is a long term data storage and retrieval engine that enables the product to receive events at high rates.

ArcSight SmartConnectors

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

SmartConnectors are not bundled with ArcSight Express and should be separately installed on a system other than the ArcSight Express appliance.

ArcSight Console

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

Deployment Overview

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

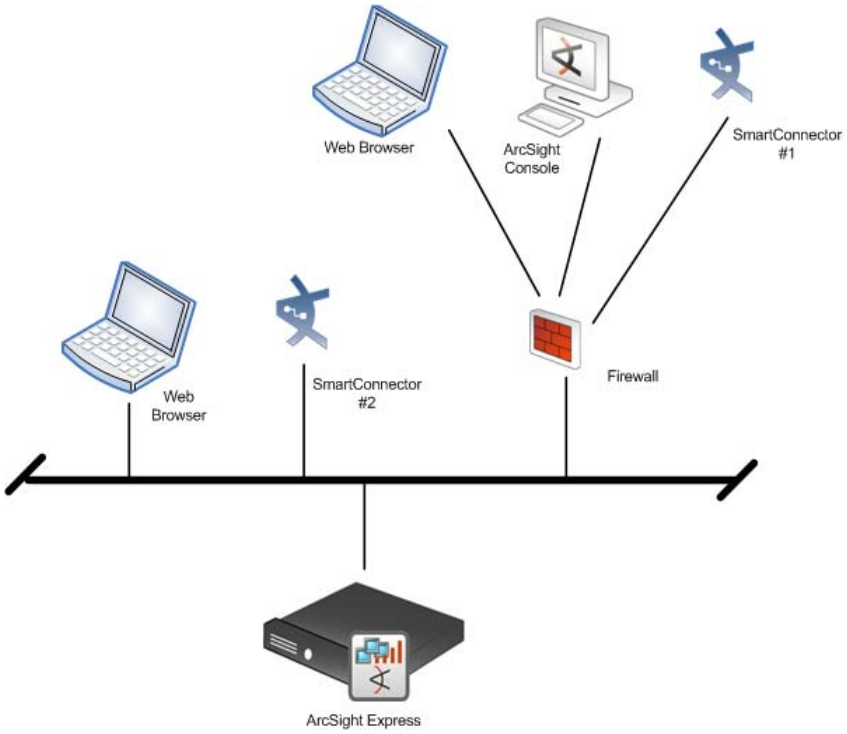


Figure 1-1 ArcSight Express Deployment

ArcSight Express v3.0 Communication Overview

ArcSight Console, ArcSight Manager, and ArcSight SmartConnector communicate using HTTP (HyperText Transfer Protocol) over SSL (Secure Sockets Layer), often referred to as

HTTPS (HyperText Transfer Protocol Secure). The HTTPS protocol provides for data encryption, data integrity verification, and authentication for both server and client.

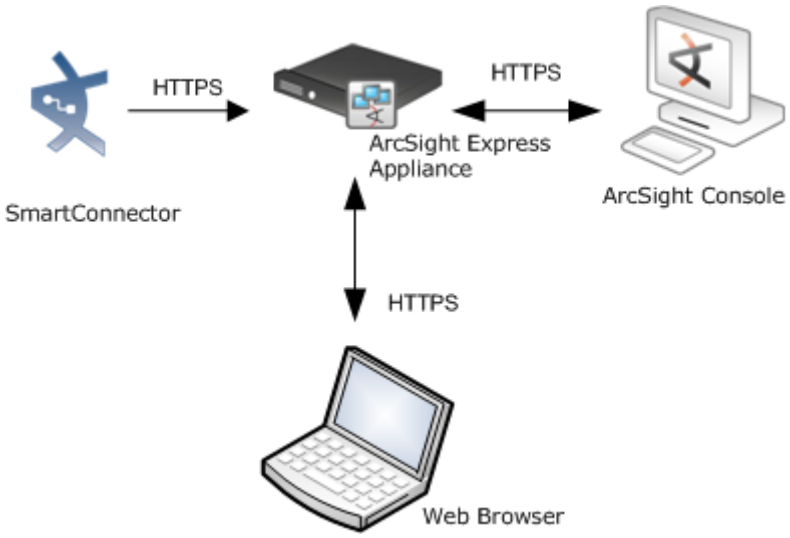


Figure 1-2 ArcSight Express v3.0 Solution - Communication

SSL works over TCP (Transport Control Protocol) connections. The default incoming TCP port on ArcSight Manager is 8443.

The Manager never makes outgoing connections to the Console or SmartConnectors. The Manager connects to the CORR-Engine on the appliance locally using JDBC.

Effect on Communication when Components Fail

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

If the CORR-Engine is unavailable for any reason, the Manager stops accepting events and caches any events that were not committed to the CORR-Engine. The SmartConnectors also start caching new events they receive, so there is no event data loss. The Console gets disconnected.

When the CORR-Engine is filled to capacity, as new events come in the ArcSight Express appliance starts deleting existing events starting from the oldest dated event.

If the Manager is unavailable, the SmartConnectors start caching events to prevent event data loss. The CORR-Engine engine is idle. The Console is disconnected.

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.

Chapter 2

Configuring the ArcSight Express v3.0 Appliance

This chapter covers the following topics:

We recommend that you read the *ArcSight Express v3.0 Release Notes* before proceeding further.

Before you Configure the Appliance

Before you begin to configure the ArcSight Express v3.0 appliance, you need to download the license zip file from the ArcSight Customer Support download site, https://arcsight.subscribenet.com.

You do not need to unzip the license zip file. The ArcSight Express v3.0 First Boot Wizard recognizes the license file in the zipped state.

Configuring the ArcSight Express v3.0 Appliance

Configuring the ArcSight Express v3.0 appliance involves:

1. Configuring the RedHat Enterprise Linux operating system installed on the appliance using the OS First Boot Wizard. The OS First Boot Wizard runs as soon as the appliance is booted. After the OS First Boot Wizard ends the system displays its login screen.
2. Configuring the software components that have been pre-installed on the appliance. This is done using the ArcSight First Boot Wizard which runs automatically after the root user logs in for the first time.

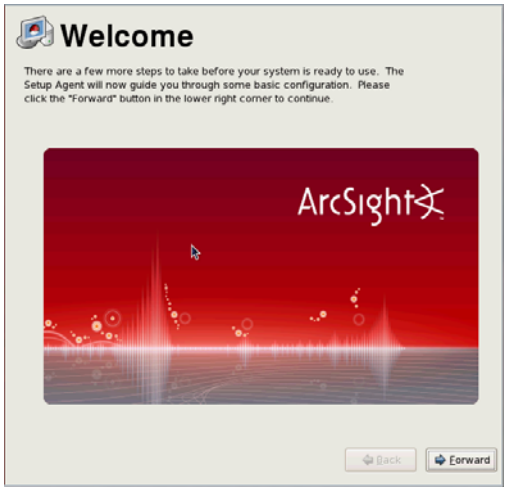
Both these wizards start automatically and run back-to-back when you boot up the appliance for the first time.

Configuring the Operating System

The ArcSight Express v3.0 appliance has the RedHat Enterprise Linux operating system installed. You have to set up the preferences for RedHat Enterprise Linux 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 RedHat Enterprise Linux:

1 Click **Forward** on the Welcome screen.



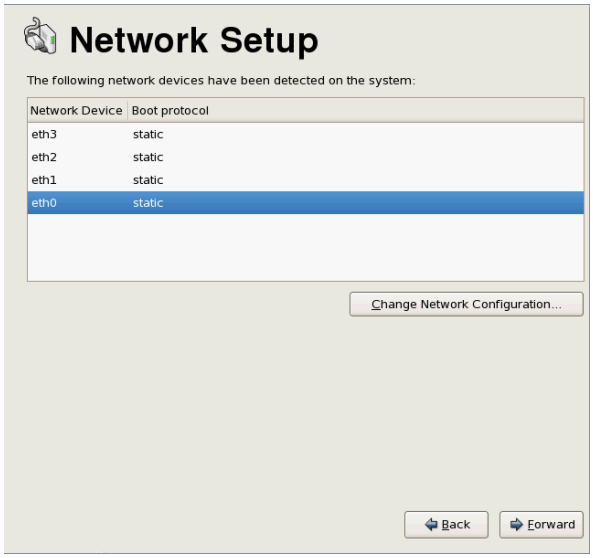
2 Read the license agreement.This license agreement is for RedHat Enterprise Linux. Select **Yes, I agree to the License Agreement** if you agree with it, and click **Forward**.

3 Select the Keyboard you will be using and click **Forward**.

4 Enter a password for the root account which is used for system administration. Re-enter to confirm it. Click **Forward**.

5 For security reasons, the Manager runs using an "arcsight" user account. The “arcsight” user account has already been created for you. Set up a password for the user “arcsight” and click **Forward**.

6 The next step is to configure the IP addresses for the appliance.

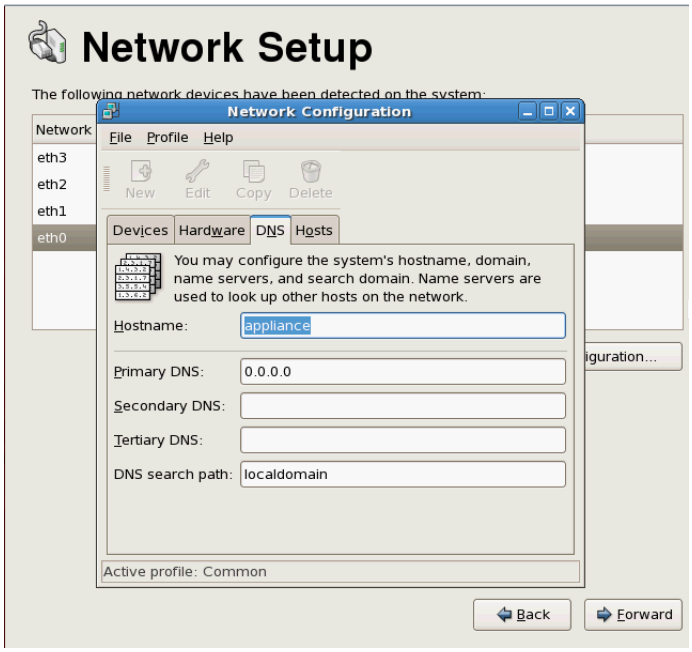


Click **Change Network Configuration...** Configure the interface of your choice.

Note

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

a Click the **DNS** tab in the Network Configuration dialog and enter a host name, DNS servers, and DNS search path (domain name) for the ArcSight Express v3.0 appliance, then click **File->Save** to save the changes. Exit the dialog.



Caution

Make sure that you do not change the default values in the Hosts tab of the Network Configuration panel shown above. If you change the default values, it could lead to loss of network connectivity and you will receive this error:

```
Could not look up internet addresses for <hostname>.This
will prevent GNOME from operating correctly.
```

b Click the **Devices** tab. To configure a network interface, select it and click the **Edit** button.

c Set the IP address, subnet mask, and default gateway in the Ethernet Device dialog and click **OK**.

Caution

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

Caution

If you want to change the host name or IP address after you have finished running this wizard, follow the steps in the sections "Changing the Host Name of the Appliance After Configuring it in the OS First Boot Wizard" on page 51 or "Changing the IP Address of the Appliance After Configuring it in the OS First Boot Wizard" on page 50 respectively.

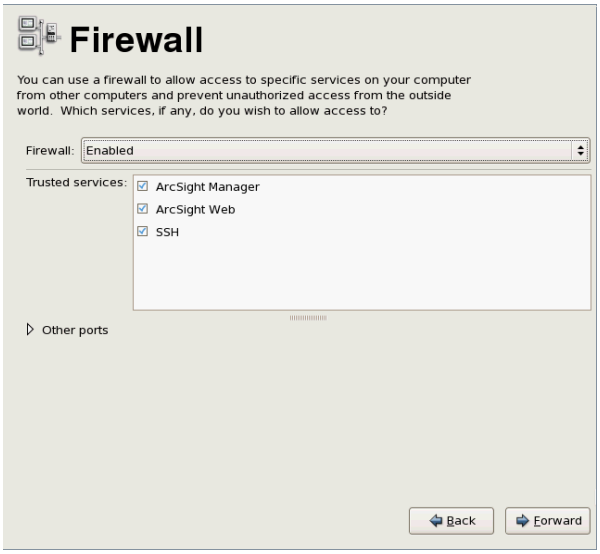
d Click **File->Save** to save the settings. If you exit the dialog without explicitly saving, you will get a prompt asking you if you want to save the changes. Click **Yes** in the Information box.

e The Network will automatically be restarted and you will see a message, "Restarting network. Please wait...".

f Click **File->Quit** to exit the Network Configuration dialog.

g Click **Forward** in the Network Setup dialog.

7 Choose **Enabled** in the Firewall dropdown menu if it is not already selected and then make sure the ports listed in the note below are open. Also add any ports you will be using to the list of Other ports by clicking the **Add** button. Click **Forward**.



Note

Make sure that the ports 8443 and 9443 are open for outgoing communications. The ArcSight Manager uses port 8443 for communication. You will also need to leave port 22 open for remote ssh access.

8 Click **Yes** in the warning dialog that follows.

9 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 Expand the **Hide advanced options** field and select **Synchronize system clock before starting service**.

d Click **Forward**. Wait for the NTP server to be contacted.

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

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

The list of servers configured by default points ArcSight Express v3.0 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.

10 On the **Timezone** panel, select the Timezone in which your ArcSight Express v3.0 appliance is located and click **Finish.**

You will be prompted to enter your username in a login screen. This begins the second phase of the First Boot Wizard which will help you configure the software components that have already been installed on your ArcSight Express v3.0 appliance.

Important!

Log in as user “root” when you are prompted with the login screen, and enter the password for this account which you had set in Step 4 on page 12. Next, you need to set up the software components on the ArcSight Express v3.0 appliance:

After you have logged in successfully, the software components configuration wizard will automatically open. Follow the directions in the section below to configure the software components on the appliance.

Configuring Software Components on the Appliance

The wizard prompts you for information required to configure the ArcSight Express v3.0 software components - ArcSight Manager and the CORR-Engine storage engine.

Restarting this wizard if you exit it...

If you exit out of any of the screens from this point forward, 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 from `/opt/arcsight/manager/bin` directory while logged in as user “root”:

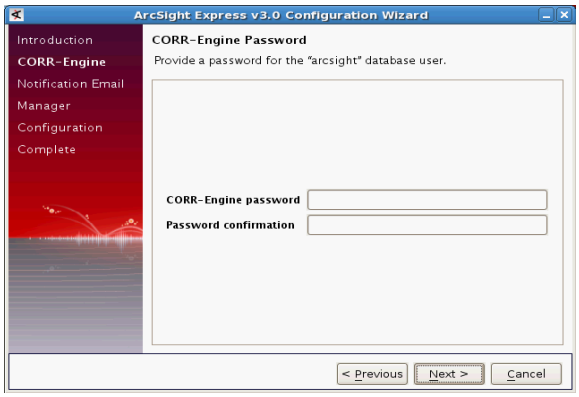
```
./arcsight appliancefirstbootsetup -boxster
```

The wizard will open the screen you see in Step 3 below.

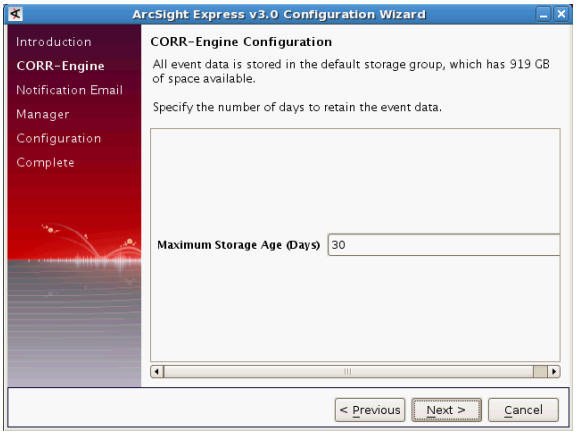
The ArcSight Express v3.0 appliance is functional only after successful completion of the wizard.

1 The software configuration wizard begins with a welcome screen. Read the welcome message and click **Next**.

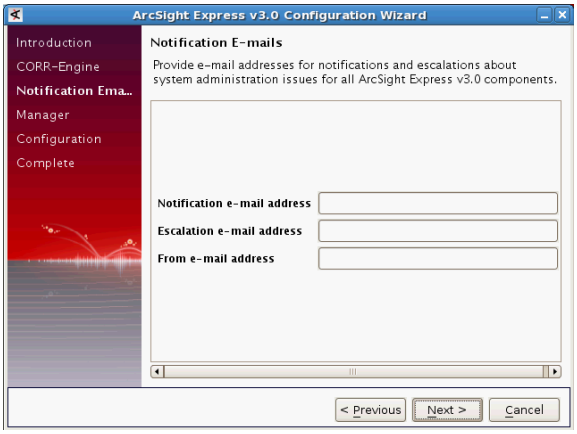
2 Set a password for your database by entering it in the Database password textbox and reentering it in the Password confirmation textbox to confirm it and click **Next**:



3 Enter the maximum number of days you would like to retain the data and click **Next**.



4 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.

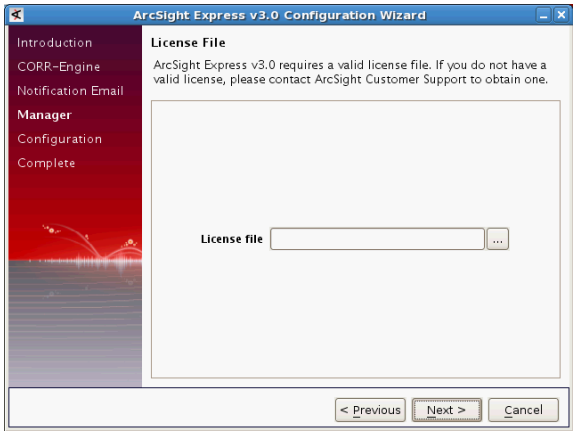
Escalation e-mail address: An e-mail address of the person who should receive an escalation e-mail in case no action has been taken for a period of time after the notification e-mail was sent.

From e-mail address: E-mail address that will be used to represent the sender of the e-mail notifications.

Click **Next**.

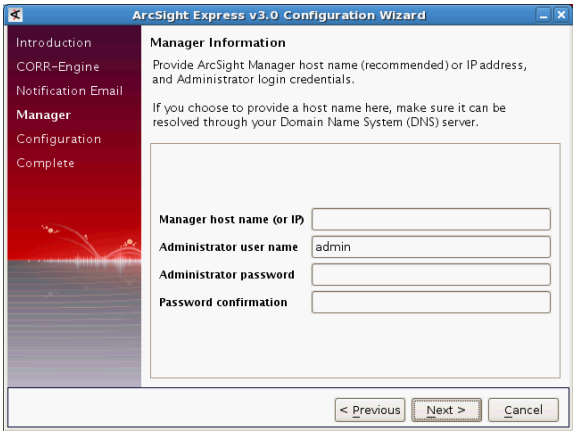
5 Enter or navigate to the location where you have stored the ArcSight Express v3.0 appliance license file and click **Next**.

If you do not have a license file, contact ArcSight Customer Support to obtain one. 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 get it onto the appliance.



6 Enter the Manager's host name, and configure information which will be used to create an ArcSight Manager user with administrative privileges. Click **Next**.

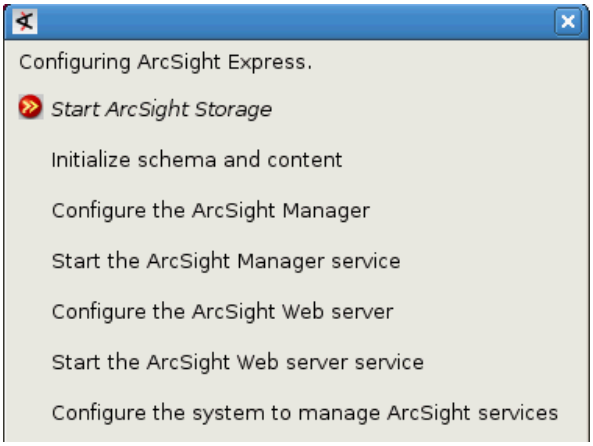
Important: Make sure to change the **Manager Host Name** to either the host name or IP address of the ArcSight Express v3.0 appliance. The Manager host name will be used to generate a self-signed certificate and also when accessing the Manager using the ArcSight Console or the Management Console. The Common Name (CN) in the certificate will be the Manager host name that you specify in the Manager Information screen.



7 You will see a screen that informs you that ArcSight Express v3.0 is ready to be configured. Click **Next** to continue with the configuration.

Keep in mind that once the wizard has started configuring the software components, if you exit the wizard or if an error occurs, you will have to configure that component manually.

8 You can see the progress and errors if any as the configuration process continues.



After the configuration completes successfully, click **Next.**

If you see a “Failed” status or exit this wizard after it has started configuring the components, but before successful completion of the wizard, you are required to manually configure the component that failed and perform the rest of the steps shown in the screen capture under Step 8 manually.

9 Once your appliance has been configured successfully, you will see a screen saying so. Click **Finish** in the Configuration Completed Successfully screen.

10 Log out of the root account by clicking **System->Log Out root**.

The ArcSight Express v3.0 appliance is ready for use.

The Next Steps

Download the ArcSight Console and install it on a supported platform. The Console should not be installed on the ArcSight Express v3.0 appliance. Refer to the next chapter, Installing ArcSight Console, for details on how to do this.

Read the *Release Notes* available on the ArcSight Customer Support download site.

Chapter 3

Running the Manager Configuration Wizard

This chapter covers the following topics:

You can change some configuration parameters on ArcSight Express v3.0 by running the `managersetup` program at any time after you have installed and configured your ArcSight Express v3.0 appliance.

Running the Wizard

We recommend running the wizard as user "arcsight". Before you run the managersetup wizard, stop your Manager by running the following command:

```
/sbin/service arcsight_services stop manager
```

Verify that the Manager has stopped by running the following command:

```
/sbin/service arcsight_services status all
```

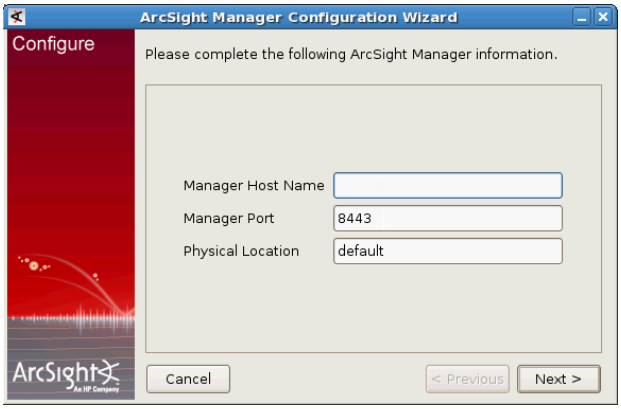
To start the `managersetup` wizard, run the following from `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

The `managersetup` wizard will start.

1 If you would like to change the hostname or IP address for your ArcSight Express v3.0 appliance, enter the host name or IP address of your ArcSight Express v3.0 machine. Keep in mind that the Manager host name that you enter in this dialog will appear on the Manager certificate. If you do change the Manager host name, be sure to

regenerate the Manager's certificate in Step 4 on page 21. We recommend that you do not change the Manager Port number.



The managersetup Configuration Wizard establishes parameters required for the Manager to start up when you boot up the ArcSight Express v3.0 appliance.

2 If you would like to replace your license file with a new one, select **Replace current license file**. otherwise accept the default option of **Keep the current license file.**

If you selected **Replace the current license file.** you will be prompted to either enter its location or navigate to the new license file.

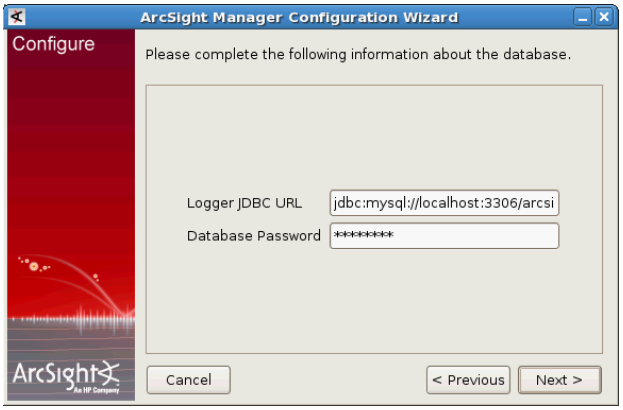
3 Select the Java Heap memory size from the dropdown menu.

The Java Heap memory size is the amount of memory that ArcSight Express v3.0 will allocate for its heap. (Besides the heap memory, the Manager on the ArcSight Express v3.0 uses some additional system memory as well.)

4 The Manager controls SSL certificate type for communications with the Console, so the wizard prompts you to select the type of SSL certificate that the Manager is using. If you had changed the Manager host name in Step 1 on page 19, select **Replace with new Self-Signed key pair**, otherwise select **Do not change anything.**

If you selected **Replace with new Self-Signed key pair**, you will be prompted to enter the password for the SSL key store and then enter details about the new SSL certificate to be issued.

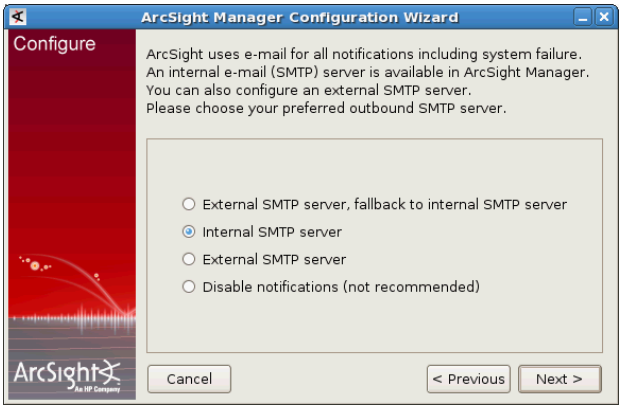
5 Accept the default in this screen and click **Next**.



6 Select the desired authentication method and click **Next**.

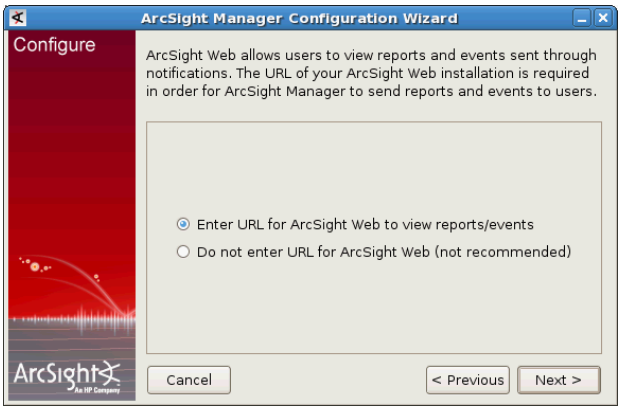
7 Select the method for authenticating the users. See “Authentication Details” on page 24 for more details on each of these options.

8 Accept the default and click **Next** or configure a different email server for notification.



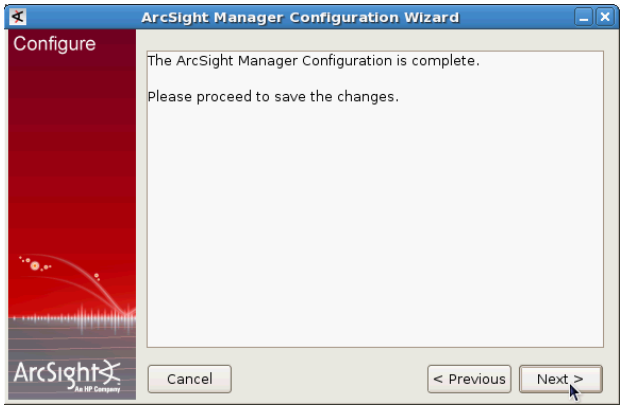
You must set up notification and specify notification recipients in order to receive system warnings. The importance of this step is sometimes overlooked, leading to preventable system failures.

9 Select **Do not enter URL for ArcSight Web** and click **Next**.



10 ArcSight Manager can automatically create an asset when it receives an event with a new sensor or device information. By default, assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation.**

11 Click **Next** in the following screen.



12 Click **Finish** in the following screen:

You have completed the Manager setup program. You can now start the Manager by running the following:

```
/sbin/service arcsight_services start manager
```

Authentication Details

The authentication options enable you to select the type of authentication to use when logging into the Manager.

- In order to use PKCS#11 authentication, you must select one of the SSL based authentication methods.
- If you plan to use PKCS #11 token with ArcSight Web, make sure to select **Password Based or SSL Client Based Authentication**.
- PKCS#11 authentication is not supported with Radius, LDAP and Active Directory authentication methods.

See the appendix "Using the PKCS#11 Token," in the *ArcSight Express Configuration Guide*, for details on using a PKCS #11 token such as the Common Access Card (CAC).

By default, the system uses its own, built-in authentication, but you can specify third party, external authentication mechanisms, such as RADIUS Authentication, Microsoft Active Directory, LDAP, or a custom JAAS plug-in configuration.

How external authentication works

The Manager uses the external authentication mechanism for authentication only, and not for authorization or access control. That is, the external authenticator only validates the information that users enter when they connect to the Manager by doing these checks:

- The password entered for a user name is valid.
- If groups are applicable to the mechanism in use, the user name is present in the groups that are allowed to access ArcSight Manager.

Users who pass these checks are authenticated.

Once you select an external authentication mechanism, all user accounts, including the admin account, are authenticated through it.

Guidelines for setting up external authentication

Follow these guidelines when setting up an external authentication mechanism:

- Users connecting to the Manager must exist on the Manager.
- User accounts, including admin, must map to accounts on the external authenticator. If the accounts do not map literally, you must configure internal to external ID mappings in the Manager.
- Users do not need to be configured in groups on the Manager even if they are configured in groups on the external authenticator.
- If user groups are configured on the Manager, they do not need to map to the group structure configured on the external authenticator.
- Information entered to set up external authentication is *not* case sensitive.

- To restrict information users can access, set up Access Control Lists (ACLs) on the Manager.

If you configure the Manager using **Password Based and SSL Client Based Authentication** or **SSL Client Only Authentication**, be aware that ArcSight Web does not support these modes. So:

- If you plan to use ArcSight Web, you will need to configure your Manager to use **Password Based Authentication** or **Password Based or SSL Client Based Authentication** as your authentication method.
- If you plan to use PKCS#11 authentication with ArcSight Web, be sure to select **Password Based or SSL Client Based Authentication** only.

Password Based Authentication

Password-based authentication requires users to enter their User ID and Password when logging in. You can select the built-in authentication or external authentication.

Built-In Authentication

This is the default authentication when you do not specify a third party external authentication method.

If you selected this option, you are done.

Setting up RADIUS Authentication

To configure ArcSight Manager for RADIUS Authentication, choose **RADIUS Authentication** and supply the following parameter values:

Parameter	Description
Authentication Protocol	Which authentication protocol is configured on your RADIUS server: PAP, CHAP, MSCHAP, or MSCHAP2.
RADIUS Server Host	Host name of the RADIUS server. To specify multiple RADIUS servers for failover, enter comma-separated names of those servers in this field. For example, server1, server2, server3. If server1 is unavailable, server2 is contacted, and if server2 is also unavailable, server3 is contacted.
RADIUS Server Type	Type of RADIUS server: • RSA Authentication Manager • Generic RADIUS Server • Safeword PremierAccess
RADIUS Server Port	Specify the port on which the RADIUS server is running. The default is 1812.
RADIUS Shared Secret	Specify the RADIUS shared secret string used to verify the authenticity and integrity of the messages exchanged between the Manager and the RADIUS server.

Setting up Active Directory User Authentication

To authenticate users using a Microsoft Active Directory authentication server, choose **Microsoft Active Directory**. Communication with the Active Directory server uses LDAP and optionally SSL.

The next panel prompts you for this information.

Parameter	Description
Active Directory Server	Host name of the Active Directory Server.
Enable SSL	Whether the Active Directory Server is using SSL. The default is True (SSL enabled on the AD server). No further SSL configuration is required for the AD server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the AD server side, not the manager.
Active Directory Port	Specify the port to use for the Active Directory Server. If the AD server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the AD server, use port 389.
Search Base	Search base of the Active Directory domain; for example, DC=company, DC=com.
User DN	Distinguished Name (DN) of an existing, valid user with read access to the Active Directory. For example, CN=John Doe, CN=Users, DC=company, DC=com. The CN of the user is the "Full Name," not the user name.
Password	Domain password of the user specified earlier.
Allowed User Groups	Comma-separated list of Active Directory group names. Only users belonging to the groups listed here will be allowed to log in. You can enter group names with spaces.

Specify any user who exists in AD to test the server connection.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the AD server.

Configuring AD SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store `<ARCSIGHT_HOME>/jre/lib/security/cacerts`, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the *Administrator's Guide*.

Setting up LDAP Authentication

The ArcSight Manager binds with an LDAP server using a simple bind. To authenticate users using an LDAP authentication server, choose **Simple LDAP Bind** and click **Next**. The next panel prompts you for this information.

Parameter	Description
LDAP Server Host	Specify the host name of the LDAP Server.

Parameter	Description
Enable SSL	Whether the LDAP Server is using SSL. The default is True (SSL enabled on the LDAP server). No further SSL configuration is required for the LDAP server. Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the LDAP server side, not the manager.
LDAP Server Port	Specify the port to use for the LDAP Server. If the LDAP server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the LDAP server, use port 389.

Specify any user who exists in LDAP to test the server connection.

Enter a valid Distinguished Name (DN) of a user (and that user's password) that exists on the LDAP server; for example, CN=John Doe, OU= Engineering, O=YourCompany. This information is used to establish a connection to the LDAP server to test the validity of the information you entered in the previous panel.

LDAP groups are not supported. Therefore, you cannot allow or restrict logging into the Manager based on LDAP groups.

If you configure your Manager to use LDAP authentication, ensure that you create users on the Manager with their Distinguished Name (DN) information in the external ID field. For example, CN=John Doe, OU= Engineering, O=YourCompany.

Specify the user name used to log in to the Manager and the External ID name to which it is mapped on the LDAP server.

Configuring LDAP SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store `<ARCSIGHT_HOME>/jre/lib/security/cacerts`, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in the *Administrator's Guide*.

Using a Custom Authentication Scheme

From the Manager Setup Wizard, you can choose the **Custom JAAS Plug-in Configuration** option if you want to use an authentication scheme that you have built. (Custom Authentication is not supported from the ArcSight Management Console.) You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.

Password Based and SSL Client Based Authentication

Your authentication will be based both upon the username and password combination as well as the authentication of the client certificate by the Manager.

Using PKCS#11 provider as your SSL Client Based authentication method within this option is not currently supported.

Password Based or SSL Client Based Authentication

You can either use the username/password combination or the authentication of the client certificate by the Manager (for example PKCS#11 token) to login if you select this option.

SSL Client Only Authentication

You will have to manually set up the authentication of the client certificate by the Manager. See the *Administrator's Guide* for details on how to do this.

You can either use a PKCS#11 Token or a client keystore to authenticate.

Chapter 4

Installing ArcSight Console

The ArcSight Console provides a user interface for you to perform administrative tasks on the ArcSight Express v3.0 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 the ArcSight Express v3.0 appliance. This chapter explains how to install and configure the ArcSight Console.

Make sure that you have successfully configured the ArcSight Express v3.0 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 Express v3.0 appliance.

Console Supported Platforms

The ArcSight Console is supported on the following operating systems.

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

Platform	Supported Operating System	JVM	Typical System Requirements
Linux	Red Hat Enterprise Linux (RHEL) 5.5 Desktop 32-bit	32-bit	x86-compatible multi-CPU system with 2-4 GB RAM
Macintosh	Macintosh OS X 10.6 64-bit	32-bit	
Windows	Microsoft Windows XP Professional SP3 32-bit Windows Vista SP2 64-bit Microsoft Windows 7 64-bit	32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM

Using a PKCS#11 Token

ArcSight Express 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.

See Appendix C, Using the PKCS#11 Token, on page 57 for details on using a PKCS #11 token with the Console.

Installing the Console

Do not install the ArcSight Console on the ArcSight Express v3.0 appliance. See the section "Console Supported Platforms" on page 29 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-5.1.0.nnnn.y-Console-Linux.bin`
Macintosh	`ArcSight-5.1.0.nnnn.y-Console-MacOSX.zip`
Windows	`ArcSight-5.1.0.nnnn.y-Console-Win.exe`

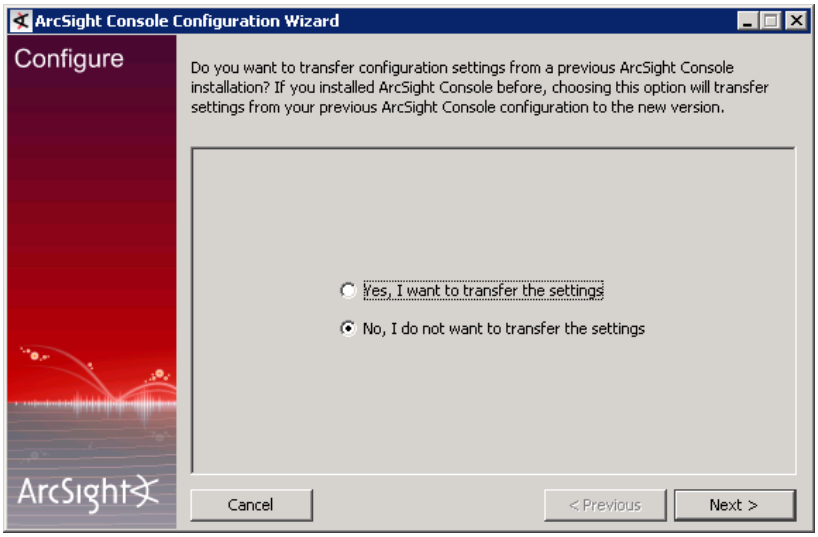
1. Click **Next** in the Installation Process Check screen.
2. Read the introductory text in the Introduction panel and click **Next**.
3. The "I accept the terms of the License Agreement" radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read 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.

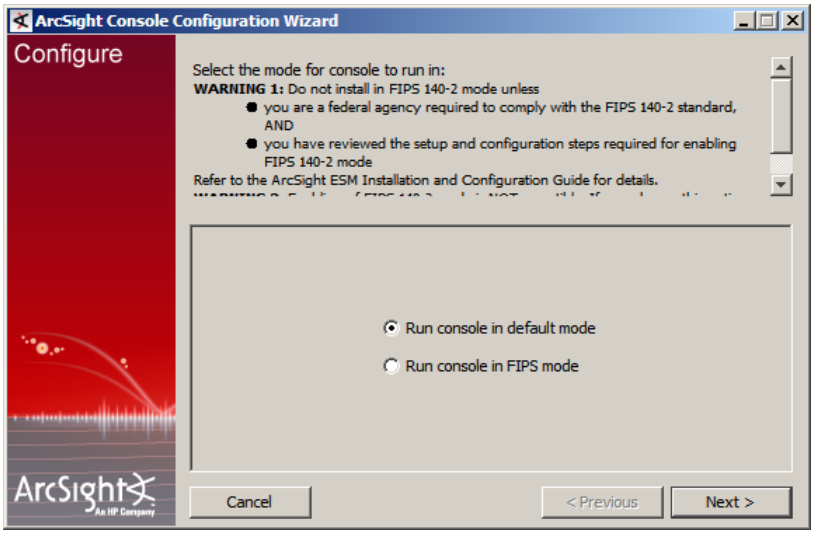


Selecting the Mode in which to Configure ArcSight Console

Note

The FIPS 140-2 mode is not supported on ArcSight Express v3.0 appliance.

Next, you will see the following screen:



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

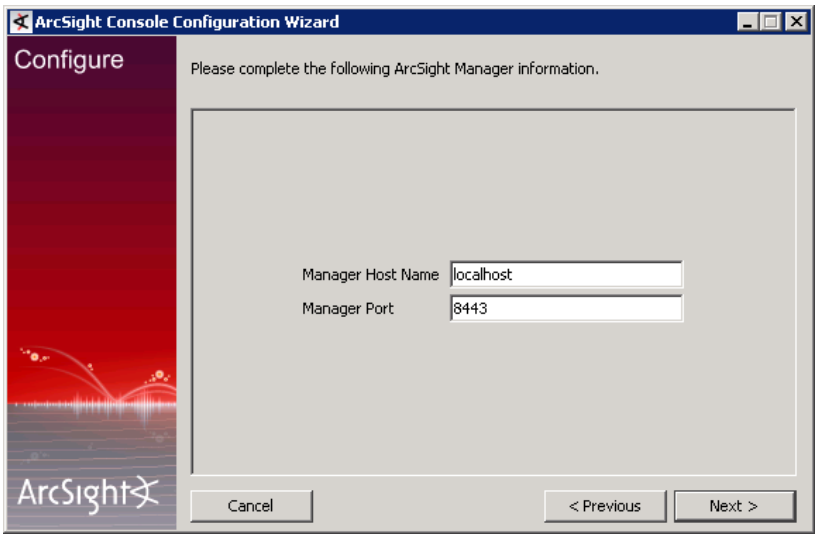
Manager Connection

The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. The hostname is the ArcSight Express v3.0 appliance host name or

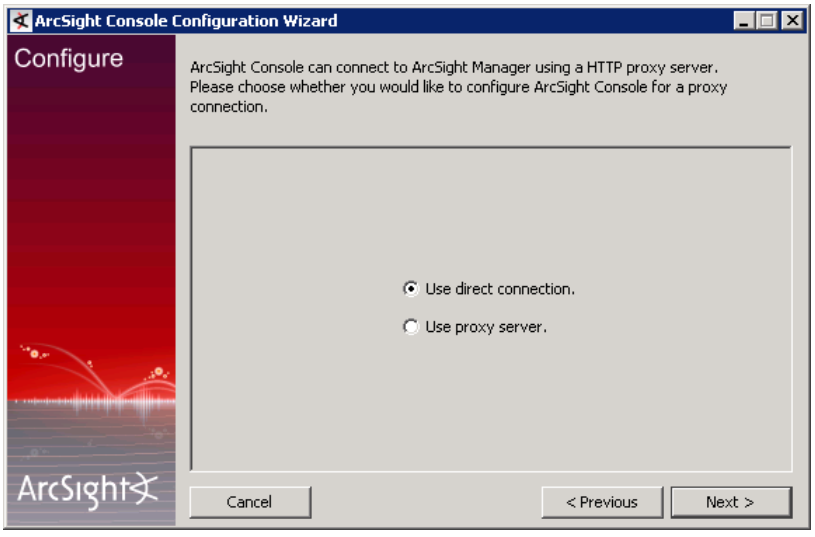
its IP address. The Manager host name that you had entered in the First Boot Wizard while configuring the ArcSight Express v3.0 appliance and the value of the Manager Host Name that you will be entering in this screen should be identical. If you had entered the machine name when configuring the First Boot Wizard, then you must enter the machine name here too, likewise, if you had entered the machine's IP address then you must enter the machine's IP address in this screen too.

Do not change the Manager's port number.

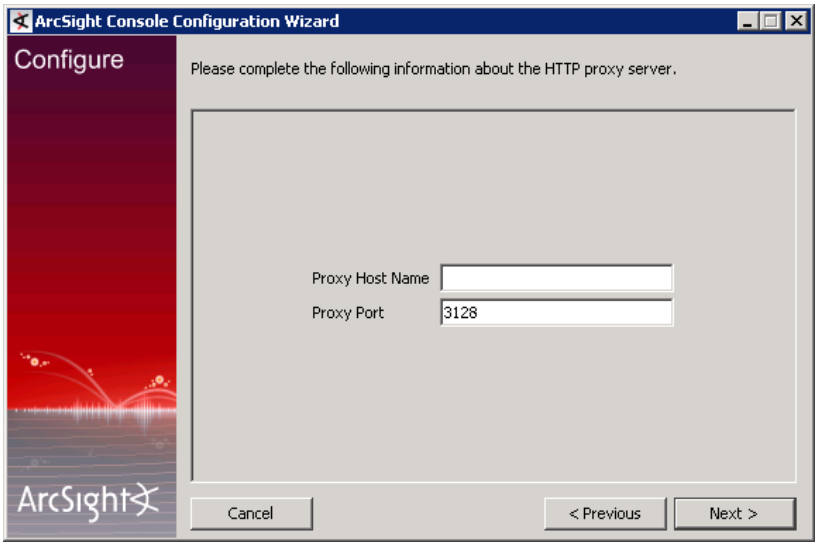
Click **Next**.



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.



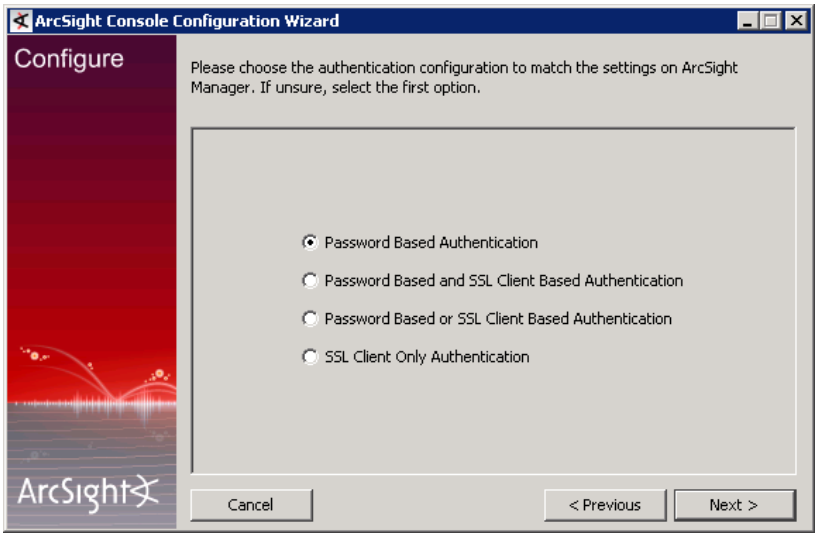
If you select the Use proxy server option, you will be prompted to enter the proxy server information.



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

Authentication

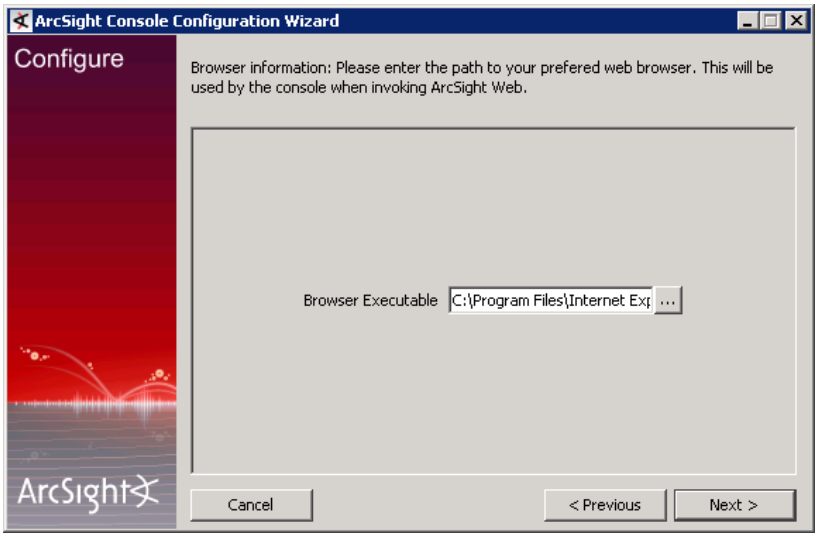
The ArcSight Console configuration wizard prompts you to choose the type of client authentication you want to use, as shown in the following screen:



Web Browser

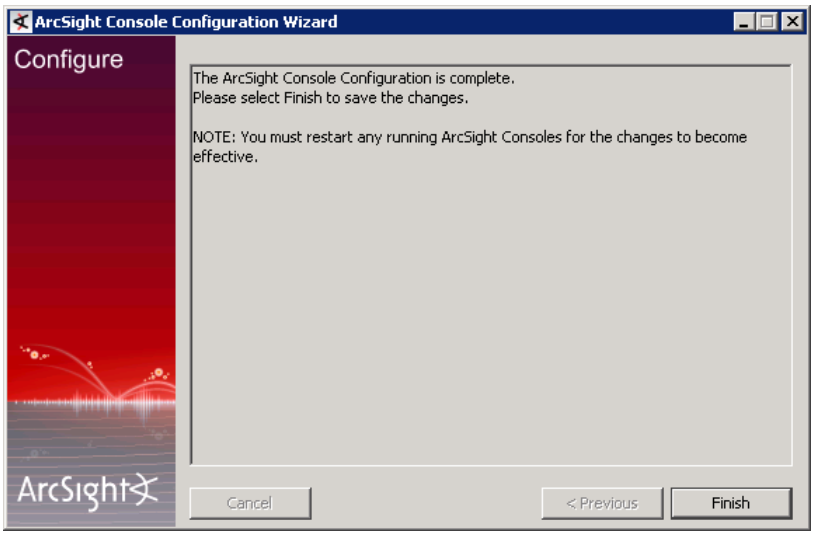
The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Base articles, and other web page content.

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 v3.0 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.

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.

Turn Off Database Recycle Bin

Turn the database recyclebin parameter off. Use the following commands:

```
prompt > arcdbutil sql
SQL>conn / as sysdba
SQL>ALTER SYSTEM set recyclebin=off scope=spfile;
```

```
SQL>shutdown immediate;
SQL>startup
SQL> show parameter recyclebin
SQL>exit
```

If you do not turn the recyclebin off you will get the following Console message:

```
The Oracle init parameter 'recyclebin' is on. ArcSight recommends
the parameter 'recyclebin' to be OFF to enable the partition
manager to correctly create reserve partitions.
```

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 Express Console 3.0**

program. If a shortcut to the Console was not installed on the Start menu, locate the Console's `UninstallerData` folder and run:

```
./Uninstall_ArcSight_Express_Console.exe
```

Chapter 5

Using SmartConnectors with ArcSight Express v3.0

This chapter covers the following topics:

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

ArcSight SmartConnectors collect a vast amount of varying, heterogeneous information. Due to this variety of information, SmartConnectors format each event into a consistent, normalized *ArcSight events*, letting you find, sort, compare, and analyze all events using the same event fields. The "normalized" events are then sent to the ArcSight Manager and are stored in the database.

Installing the SmartConnector

Installing and configuring the SmartConnector is a three step process:

1. Install the SmartConnector.

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

2. Import the Manager's certificate to the Connector's truststore. See the section Importing the Manager's Certificate for details on how to do this.

3. Configure the SmartConnector.

   For complete configuration instructions for a particular SmartConnector, see the configuration guide for that connector. The product-specific configuration guide provides specific device configuration information, installation parameters, and device event mappings to the ArcSight Express v3.0 fields.

Importing the Manager's Certificate

You will be required to import the Manager's certificate manually:

- Use the `keytoolgui` tool. See the *Administrator's Guide* for ArcSight Express v3.0 for details on importing the Manager's certificate using the `keytoolgui`.

Using keytoolgui to Import Manager's Certificate

You will need to export the Manager's certificate from the ArcSight Express v3.0 Appliance before you can import it on the Smart Connector in the Smart Connector server.

Exporting the Manager's Certificate

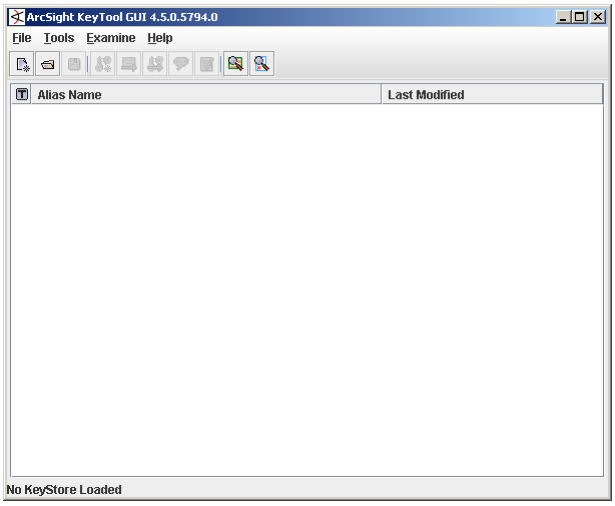
To export the Manager's certificate:

a Open a shell/command prompt window on the ArcSight Express v3.0 Appliance.

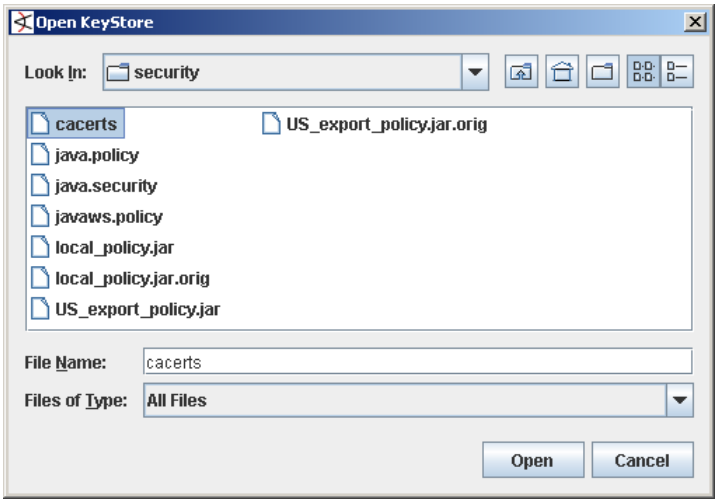
b Run the following command from the ArcSight Express v3.0 Manager's `/opt/arcsight/manager/bin` directory while logged in as user "arcsight":

```
./arcsight keytoolgui
```

The keytoolgui interface will open.

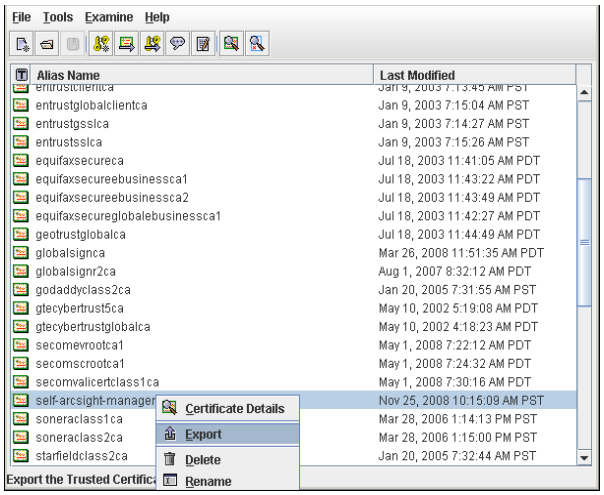


c Select **File->Open KeyStore** from the menu and navigate to the Manager's truststore (`cacerts`) located in `/opt/arcsight/manager/jre/lib/security/` directory.

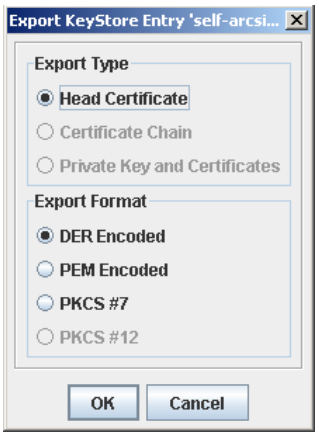


d Enter the keystore password. The default password is “changeit” (without the quotes).

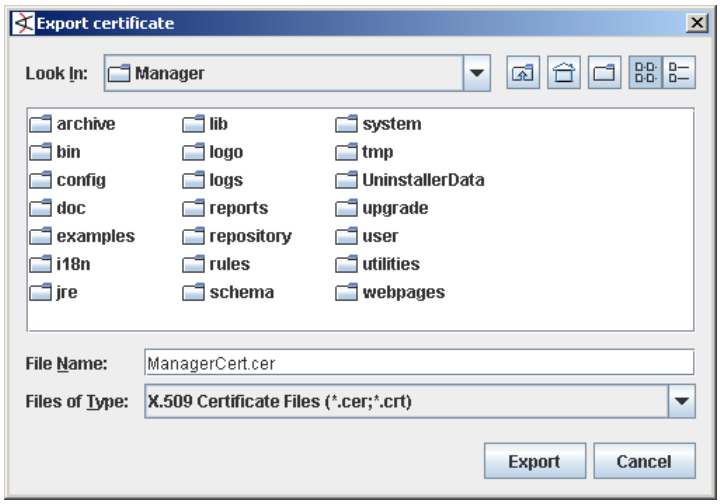
e Right-click the Manager’s certificate as shown below and select **Export**.



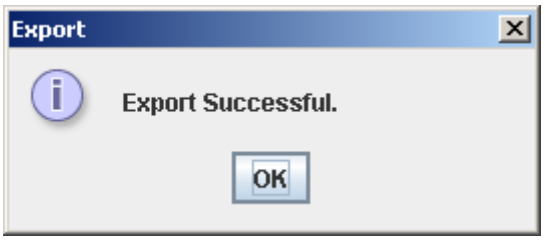
f Accept the default settings in the following dialog and click **OK**.



g Navigate to the location where you want to export the certificate and enter a file name in the File Name text box when naming the certificate and click **Export**.



h You will see the following prompt when the certificate is exported successfully.



i Click **OK** and exit the `keytoolgui`.

j Transfer (or scp) this exported certificate file from the ArcSight Express v3.0 Appliance to the Smart Connector server where you will be importing it into the SmartConnector.

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

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

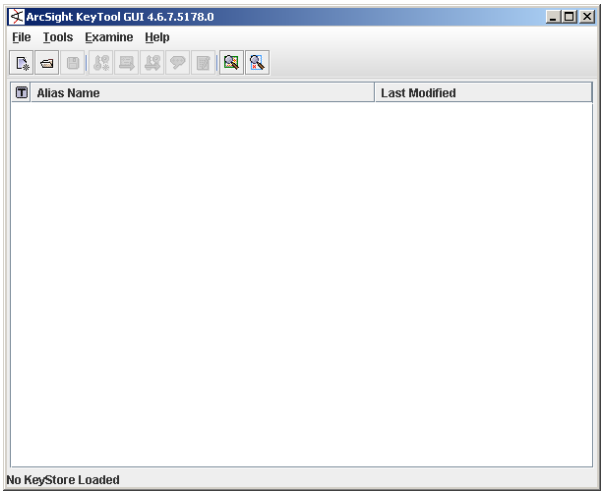
To do so:

a Open a shell/command prompt window on the SmartConnector server.

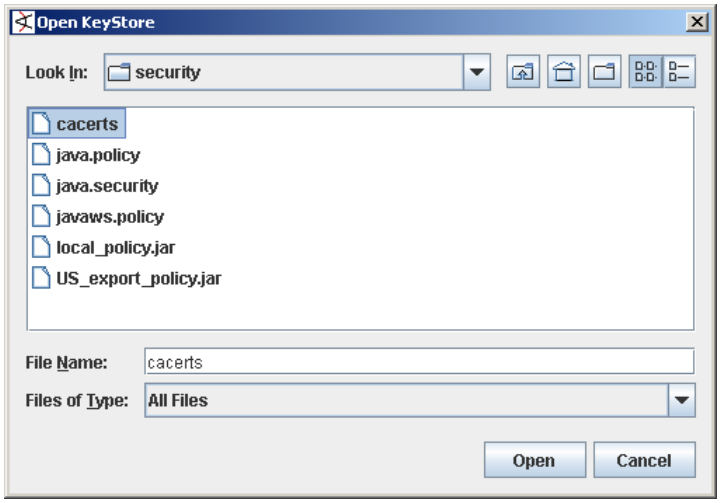
b Run the following command from the Connector's `/opt/arcsight/connector/current/bin` directory while logged in as user "arcsight":

```
./arcsight agent keytoolgui
```

The keytoolgui interface will open.

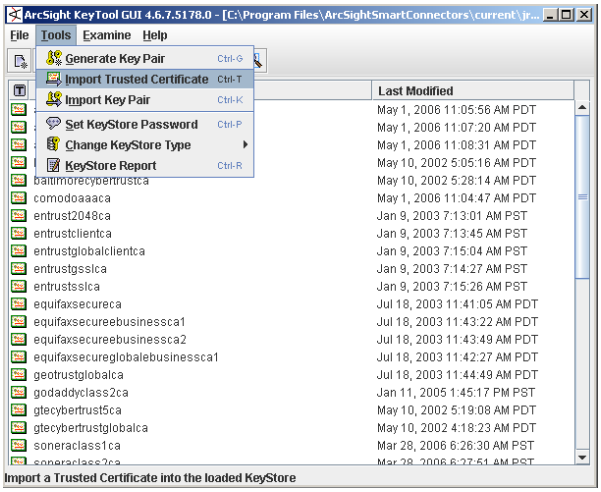


c Select **File->Open KeyStore** from the menu and navigate to the Connector's truststore (`cacerts`) located in `/opt/arcsight/connector/current/jre/lib/security/` directory.

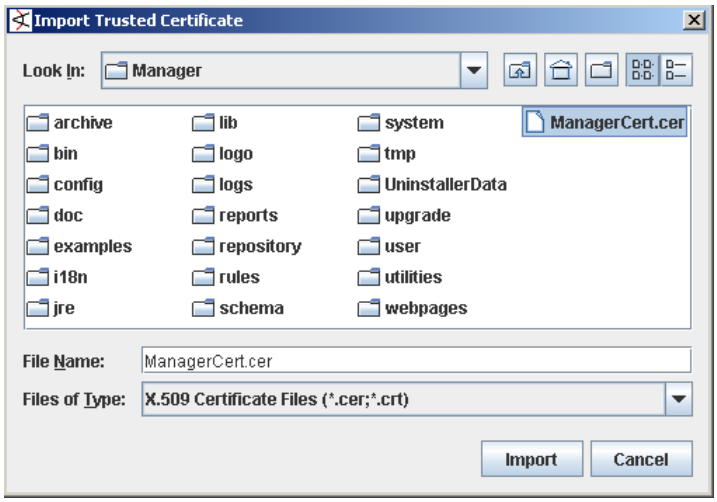


d Enter the password. The default password is "changeit" (without the quotes).

e Click **Tools->Import Trusted Certificate**.



f Navigate to the Manager's certificate, select it and click **Import**.



g You will see the following prompt. Click **OK** to see the certificate details.

The **Certificate Details** dialog will be displayed.

h Click **OK** on the **Certificate Details** dialog to accept the certificate.

i Click **Yes** in the following dialog.

j Enter an alias for the certificate and click **OK**.

k You will see the following message when the import is successful.

Click **OK**.

l Click **File->Save KeyStore** to save the certificate in the Connector's truststore and exit the `keytoolgui` interface.

Appendix A
Troubleshooting

The following information may help solve problems that might occur when installing or using ArcSight Express. In some cases, the solution can be found here or in other ArcSight Express documentation, but ArcSight Customer Support is available if you need it.

This chapter covers the following topics:

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

Location of Log files for Components

The log files can be found in the following location:

Log file name	location	Description
First Boot Wizard Logs		
fbwizard.log	`/opt/arcsight/manager/logs/default/`	Contains detailed troubleshooting information logged during the steps in "Configuring Software Components on the Appliance".

Log file name	location	Description
appliancefirstbootsetup.log	/opt/arcsight/manager/logs/	Contains brief troubleshooting information about commands that ran during the steps in "Configuring Software Components on the Appliance".
Manager Log Files		
server.log	/opt/arcsight/manager/logs/default	Contains troubleshooting information about the Manager running on the appliance
server.std.log	/opt/arcsight/manager/logs/default	Contains the stdout output of the Manager
server.status.log	/opt/arcsight/manager/logs/default	Contains a dump of all the MBeans, the memory status, thread status, etc.
CORR-Engine Log Files		
logger_server.log	/opt/arcsight/logger/current/arcsight/logger/logs	Contains troubleshooting information about the CORR-Engine running on the appliance
logger_server.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engine stdout log file
ArcSight Web Log Files		
webserver.log	/opt/arcsight/web/logs/default	Contains troubleshooting information about ArcSight Web running on the appliance
webserver.std.log	/opt/arcsight/web/logs/default	Contains the stdout output of ArcSight Web
server.status.log	/opt/arcsight/web/logs/default	Manager status moniting log file
Log file for services		
arcsight_services.log	/opt/arcsight/services/logs/	Contains information from commands that manage ArcSight service processes.

Log file name	location	Description
monit.log	/opt/arcsight/services/monit/data/	Contains timing information from startup and shutdown of ArcSight service processes.

Customizing ArcSight Express Components Further

The First Boot Wizard configures the software components on the appliance (ArcSight Manager and the CORR-Engine Storage) 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 Manager

1. Stop the Manager if it is running:

   ```
   /sbin/service arcsight_services stop manager
   ```

2. While logged in as user “arcsight”, run the following command from `/opt/arcsight/manager/bin` directory:

   ```
   ./arcsight managersetup
   ```

3. Follow the prompts on the wizard screens.

4. Restart the Manager after the wizard completes by running:

   ```
   /sbin/service arcsight_services start manager
   ```

ArcSight Web

1. Stop ArcSight Web if it is running:

   ```
   /sbin/service arcsight_services stop arcsight_web
   ```

2. While logged in as user “arcsight”, run the following command from `/opt/arcsight/web/bin` directory:

   ```
   ./arcsight webserversetup
   ```

3. Follow the prompts on the wizard screens.

4. Restart ArcSight Web after the wizard completes by running:

   ```
   /sbin/service arcsight_services start arcsight_web
   ```

Fatal Error when Running the First Boot Wizard

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

To resolve this issue, try the following steps:

1. Check the `/opt/arcsight/manager/logs/fbwizard.log` file to figure out where the error occured.

2 Check to make sure that the IP address for the appliance has been configured correctly (eth0 has been configured correctly) and is available (not already in use for some other system on your network).

3 Restart the First Boot Wizard by running the following command from the `/opt/arcsight/manager/bin` directory when logged in as user “root”:

```
./arcsight appliancefirstbootsetup -boxster
```

The First Boot Wizard can only be rerun if it did not reach the point where it configures the Manager.

If the steps above do not solve the issue, you will be required to revert your appliance to its factory settings. For instructions on how to do this, see Appendix D, Restoring Factory Settings, on page 67.

Changing the IP Address of the Appliance After Configuring it in the OS First Boot Wizard

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

Please note, that the Manager setup command must be run when logged in as user “arcsight.”

1 Stop all ArcSight services by running:

```
/sbin/service arcsight_services stop all
```

2 Change the IP address of the appliance in the `/etc/sysconfig/networkscripts/ifcfg-eth0` file.

3 Reboot the appliance.

Only if you had entered an IP address (instead of a host name) when setting up the Manager in the ArcSight First Boot Wizard do the following additional steps:

4 Stop the Manager and ArcSight Web again. (They would have automatically started upon reboot.)

To stop the Manager, run:

```
/sbin/service arcsight_services stop manager
```

To stop the ArcSight Web, run:

```
/sbin/service arcsight_services stop arcsight_web
```

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

```
./arcsight managersetup
```

This will open the Manager’s setup wizard.

a. Enter the new IP address (that you set for your appliance in Step 2 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.

6. Start the Manager by running:

```
/sbin/service arcsight_services start manager
```

7. Export the the Manager's newly generated self-signed certificate and import it into ArcSight Web using the `keytoolgui` tool. See the *Administrator's Guide* for details on how to export and import a certificate. See the "Using Keytoolgui to Export a Certificate" and "Using Keytoolgui to Import a Certificate" sections in the "Configuration" chapter in the *Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

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

```
./arcsight websetup
```

a. Enter the new IP address (that you set for your appliance in Step 2 above) in Webserver Host Name field when prompted.

b. Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new IP address.

9. Start ArcSight Web by running:

```
/sbin/service arcsight_services start arcsight_web
```

10. Import the Manager's newly generated certificate on all clients (Console and connectors) that will be accessing the Manager. You can do so using the keytoolgui. See the "Using Keytoolgui to Import a Certificate" section in the "Configuration" chapter in the *Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

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

Changing the Host Name of the Appliance After Configuring it in the OS First Boot Wizard

Please note that the Manager setup command must be run when logged in as user "arcsight."

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

1. Stop all services by running:

```
/sbin/service arcsight_services stop all
```

2. Change the host name to the new host name in the Network Administration tool on your appliance:

   a. Run the graphical Network Administration tool by selecting **System->Administration->Network** or entering `system-config-network` at a shell prompt.

   b. In the Network Configuration window, click the **DNS** tab.

   c. Change the host name in the Hostname textbox.

   d. Click **File->Save**, then exit the dialog.

3. Reboot the appliance.

If you had entered a host name (instead of an IP address) when configuring the Manager in the ArcSight First Boot Wizard, then you will be required to do the following in addition to the steps mentioned above:

4. Stop the Manager by running:

   ```
   /sbin/service arcsight_services stop manager
   ```

5. Stop ArcSight Web by running:

   ```
   /sbin/service arcsight_services stop arcsight_web
   ```

6. Run the Manager's setup program from the `/opt/arcsight/manager/bin` directory as user "arcsight":

   ```
   ./arcsight managersetup
   ```

   a. Enter the new host name (that you set for your appliance in the steps 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 host name.

7. Start the Manager by running:

   ```
   /sbin/service arcsight_services start manager
   ```

8. Export the the Manager's newly generated self-signed certificate and import it into ArcSight Web using the `keytoolgui` tool. See the "Using Keytoolgui to Export a Certificate" and "Using Keytoolgui to Import a Certificate" sections in the "Configuration" chapter in the *Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

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

   ```
   ./arcsight websetup
   ```

   a. Enter the new host name in Webserver Host Name field when prompted.

   b. Select the self-signed keypair option when prompted by the wizard and enter the required information to generate the self-signed certificate containing the new hostname.

10. Start ArcSight Web by running:

    ```
    /sbin/service arcsight_services start arcsight_web
    ```

11 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 the "Using Keytoolgui to Import a Certificate" section in the "Configuration" chapter in the *Administrator's Guide* available on the ArcSight Customer Support download site for details on how to do this.

12 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 v3.0. It covers the default settings for the following:

You can always customize any component by running its setup program.

The following tables list the default settings for each component.

General

Setting	Default Value
default password for Java keystore	changeit

ArcSight Manager

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

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

Setting	Default Value
Location of Manager	/opt/arcsight/manager
Manager host name	Host name or IP address of ArcSight Express
Manager Port	8443
Manager license file	Please obtain from ArcSight Customer Support
Packages installed	All system content packages
Java Heap Memory	8 GB

Setting	Default Value
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,
	1 Stop the Manager by running the following command:
	`/sbin/service arcsight_services stop manager`
	2 Run the following command from the `/opt/arcsight/manager/bin` directory and set up the external SMTP server when prompted:
	`./arcsight managersetup`
	3 Start the Manager by running:
	`/sbin/service arcsight_services start manager`

Sensor Asset Auto Creation	Enabled
Packages/default content installed	All system content
Manager installed as service	No

Appendix C

Using the PKCS#11 Token

This appendix covers the following topics:

ArcSight ESM supports the use of a PKCS#11 token, such as the Common Access Card (CAC), which is used for identity verification and access control. The PKCS#11 token authentication works using the SSL client-side authentication.

PKCS#11 authentication is not supported with Radius, LDAP and Active Directory authentication methods.

What is PKCS?

Public Key Cryptography Standards (PKCS), published by RSA Laboratories, comprises of a group of standards used for reliable and secure public key cryptography. Public Key Cryptography works by encrypting the data at the sender's end and decrypting it at the receiver's end.

PKCS#11

PKCS#11, one of the PKCS standards, is an API defining a generic interface to cryptographic tokens, software tokens and hardware tokens such as hardware security modules and smartcards. A cryptographic token is a security device that is used to authorize the use of the software or hardware, such as the smartcard or Common Access Card (CAC). The credentials of the authorized user are stored on the hardware itself. ESM uses the PKCS#11 interface provided by the Network Security Services (NSS) cryptographic module to communicate with it (the NSS cryptographic module). The use of PKCS #11 is an example of client-side authentication.

PKCS#12

PKCS#12, also a PKCS standard, defines a file format, the .pfx file format, which is used to store private keys and their accompanying public key in a single encrypted file in the NSS DB. The .pfx files are password protected. Key pairs stored in NSS DB are required to be stored in this format. When ArcSight Web and Manager are configured to run in FIPS

mode, their key pairs are stored in the .pfx format in their NSS DB. PKCS #12 is applicable to server-side authentication.

PKCS#11 Token Support in ArcSight Express v3.0

ArcSight Express v3.0 supports any PKCS#11 Token vendor that supports PKCS#11 2.0 or above. You have to make sure that:

The vendor's driver and the PKCS#11 driver DLL are installed on the machine on which you plan to use the PKCS#11 token.

Before you use the PKCS#11 token, make sure that you have installed the provider software on the system where you have installed the Console or Web with which you plan to use the PKCS#11 token. Refer to your PKCS#11 token provider's documentation on how to install and configure your cryptographic device.

To use a PKCS #11 token, make sure that the token's CA's root certificate is imported into the Manager's and Web's (if you plan to use CAC with Web) truststore. You also have to map the CAC card's CN to the External User ID in the Console.

An Example - Using the ActivClient CAC Card

Even though ArcSight Express v3.0 supports authentication through any PKCS#11 token, in this appendix, we will discuss in detail how to use the ActivClient's Common Access Card (CAC) as an example.

Using CAC with ArcSight Console

To use CAC with the Console:

Install the CAC Provider's Software

Before you use the Common Access Card (CAC), make sure that you have installed its software on the system where you have installed the Console with which you plan to use CAC. Refer to your CAC provider's documentation on how to install and configure it.

Map a User's External ID in the Manager to the CAC's Subject CN

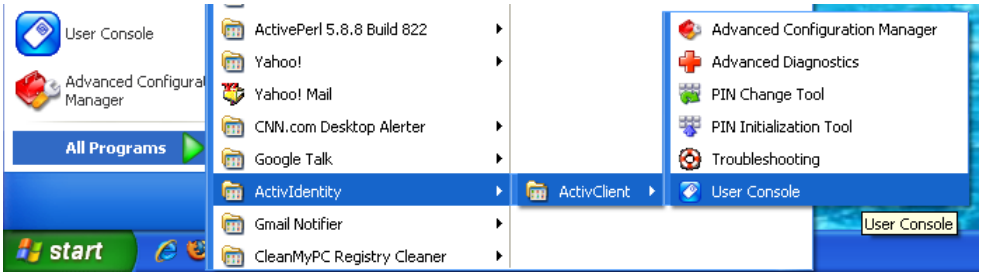
You are required to map the Common Name (CN) on the CAC to a User's External ID on the Manager. This allows the Manager to know which of its user is being represented by the identity stored in the CAC card.

The CAC card contains three types of certificate, Signature, Encryption and ID certificates. Only ID certificate is supported.

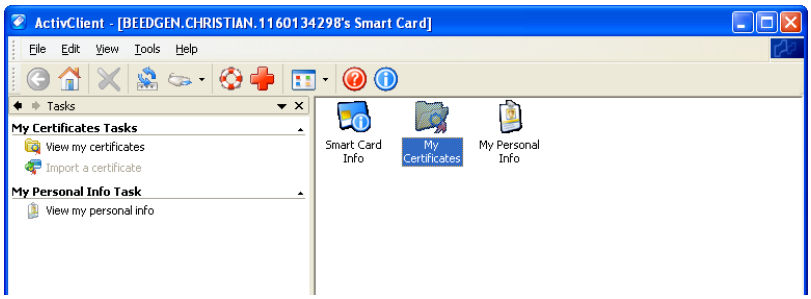
1 Obtain the Subject CN from the CAC card.

   a Insert the CAC card into the reader if not already inserted.

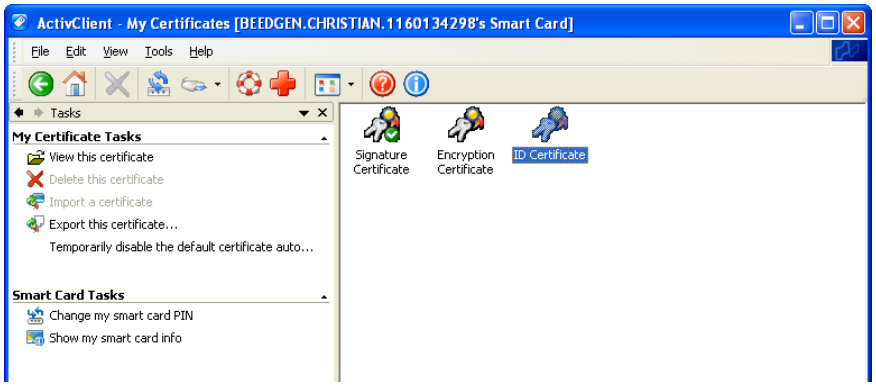
b Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



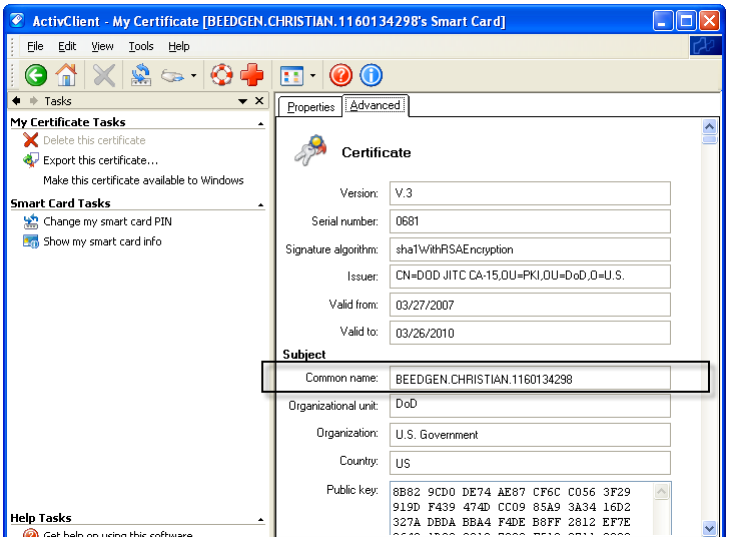
c Double-click **My Certificates** in the following screen:



d Double click **ID Certificate** in the following screen:



e Click on the **Advanced** tab and copy the contents in the Common name text box. You will have to copy it by hand on to a sheet of paper. Using the context menu to copy is not supported.



2 In ArcSight Console, map the User's External ID to the CAC card CN:

a In the Console, double-click the user whose External ID you want to map to the CAC card common name. This will open the Inspect/Edit pane for that user.

b Enter the CN you obtained in the previous step into the **External User ID** field and click **Apply**.

Obtain the CAC's Certificate

PKCS#11 Token authentication is based on SSL client-side authentication. In the case of the Common Access Card, the key pair for the client (the CAC device) is stored within the card itself.

Option 1:

You can obtain the CAC card's certificate signer's root CA certificate from the PKI administrator.

or

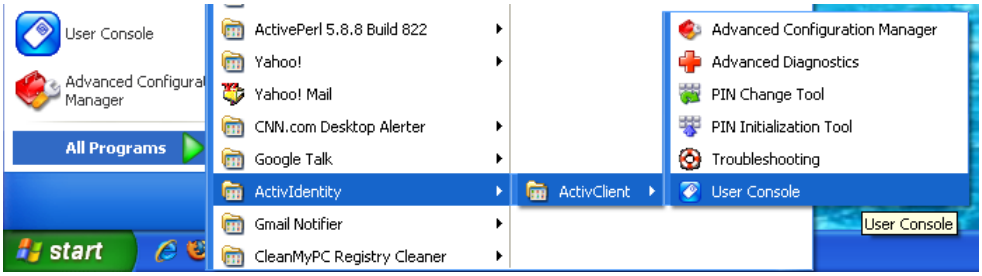
Option 2:

You can export the CAC card's certificate from its keystore and then extract the root CA certificate from this certificate.

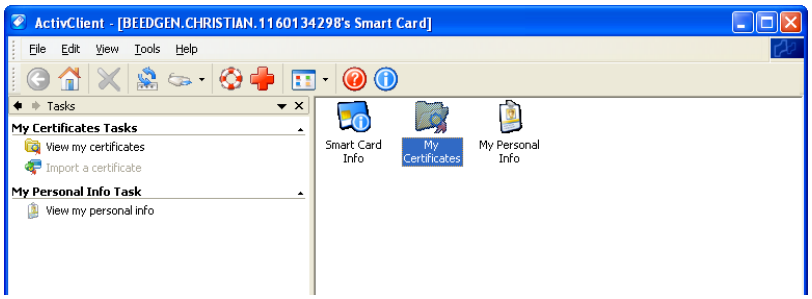
The steps to extract the CAC card's certificate from the card are:

1 Insert the CAC card into the reader if not already inserted.

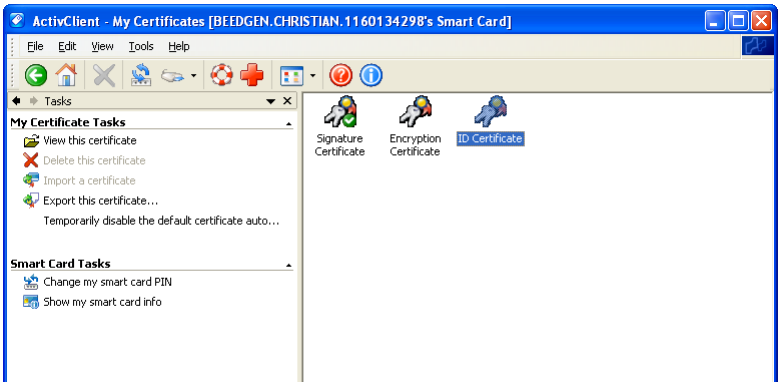
2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



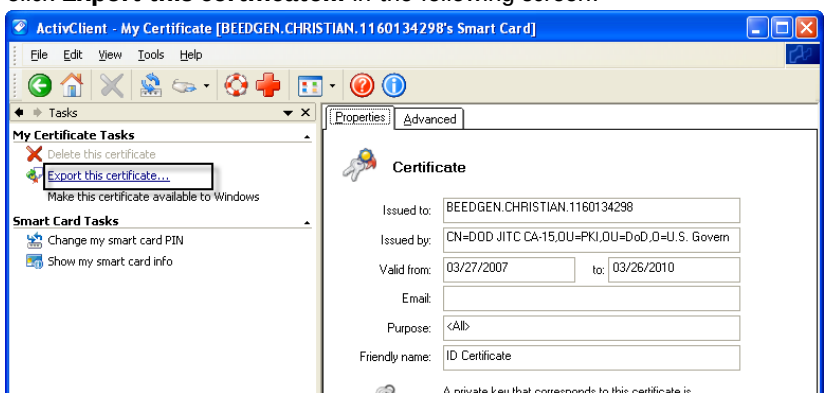
3 Double click **My Certificates** in the following screen:



4 Double click **ID Certificate** in the following screen:



5 Click **Export this certificate...** in the following screen:



6 Enter a name for the certificate in the **File name** box and navigate to a location on your machine where you want to export it to and click **Save**.

7 You will see the following status:

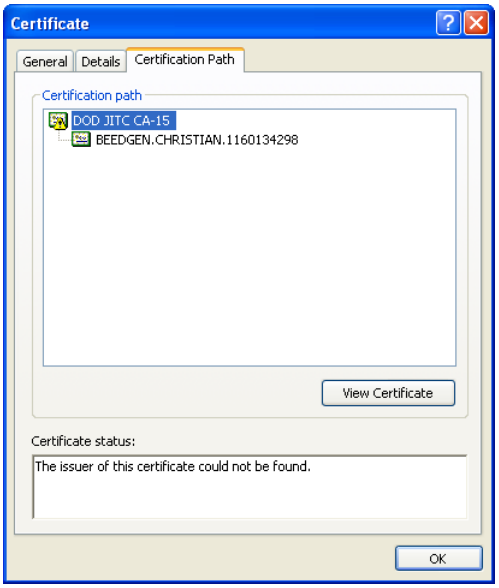
8 Exit the ActivClient window.

Extract the Root CA Certificate From the CAC Certificate you Exported

This step is required because you are required to import the CAC card certificate signer's CA root certificate into the Manager's `nssdb` and ArcSight Web's `webnssdb` (if planning to use CAC with ArcSight Web).

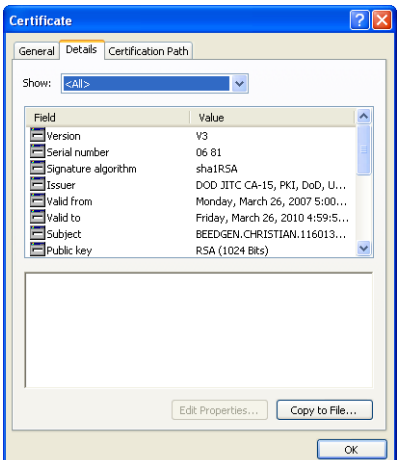
1 Double-click the CAC's certificate that you exported. The Certificate interface will open.

2 Click the **Certification Path** tab and select the root certificate as shown in the example below:



3 Click **View Certificate**.

4 Click the **Details** tab and click **Copy to File..**.



5 The Certificate Export Wizard will open. Follow the prompts in the wizard screens and accept all the defaults.

6 Enter a name for the CAC root CA certificate file when prompted and continue with the wizard by accepting all the defaults. The certificate gets exported to the same location as the CAC certificate from which you extracted it.

7 Exit the Certificate dialog.

Import the CAC Card's Root CA Certificate into the Manager's Truststore

You are required to import the CAC card's root CA certificate into the Manager's <ARCSIGHT_HOME>/config/jetty/truststore directory. For details on how to do this, see the *Administrator's Guide* for ArcSight Express v3.0.

Select Authentication Option in Manager Setup

Make sure that the authentication on the Manager is set to **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication** on the Manager.

The authentication option you select on the Manager has to match the authentication option on ArcSight Web.

So, if you plan to use PKCS#11 token with ArcSight Web, keep in mind that ArcSight Web does not support the **SSL Client Only Authentication** method. So, make sure you select **Password Based or SSL Client Based Authentication** option.

To set the authentication option on the Manager:

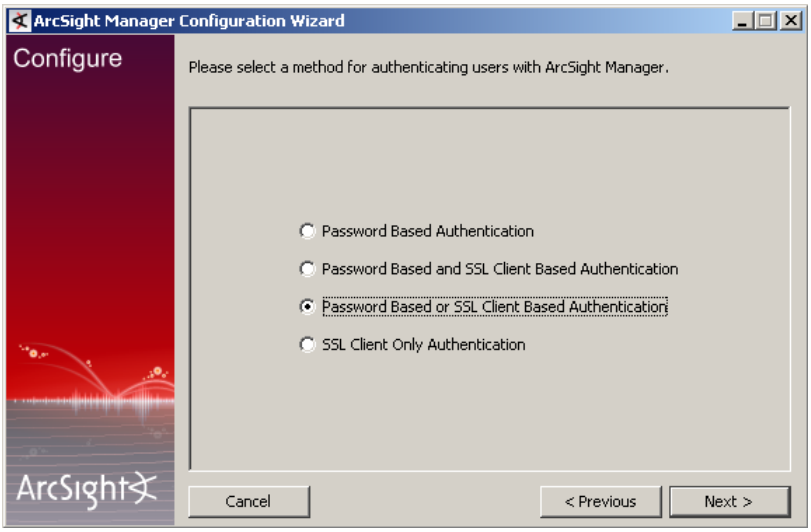
1 Stop the Manager by running the following command on the ArcSight Express Appliance:

```
/sbin/service arcsight_services stop manager
```

2 Run the following command from the `/opt/arcsight/manager/bin` directory:

```
./arcsight managersetup
```

3 Select **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication** in the following screen.



4 Complete the setup by following the prompts in the next few screens.

5 Start the Manager by running:

```
/sbin/service arcsight_services start manager
```

Select Authentication Option in Console Setup

The authentication option on the Console should match the authentication option that you set on the Manager. Run the Console setup program and either confirm or change the authentication on the Console to match that of the Manager. To do so:

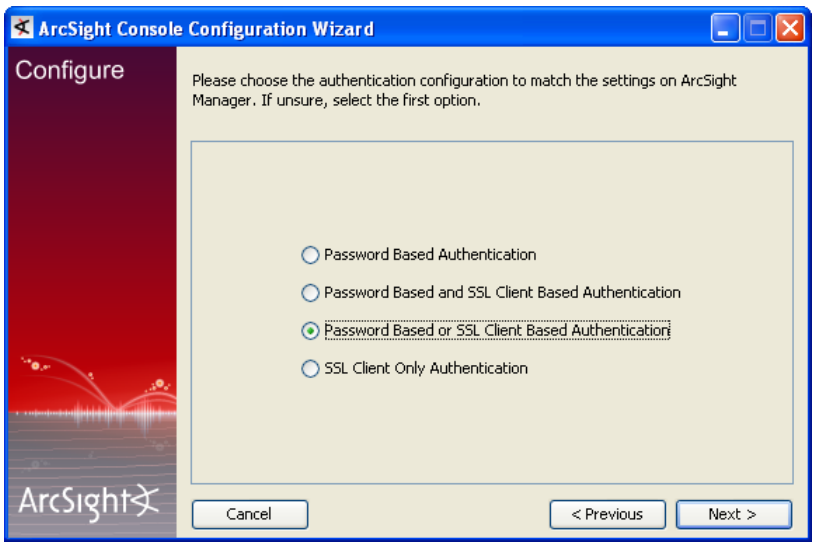
1 Stop the Console if it is running.

2 Run the Console's setup program from the Console's `bin` directory:

```
arcsight consolesetup
```

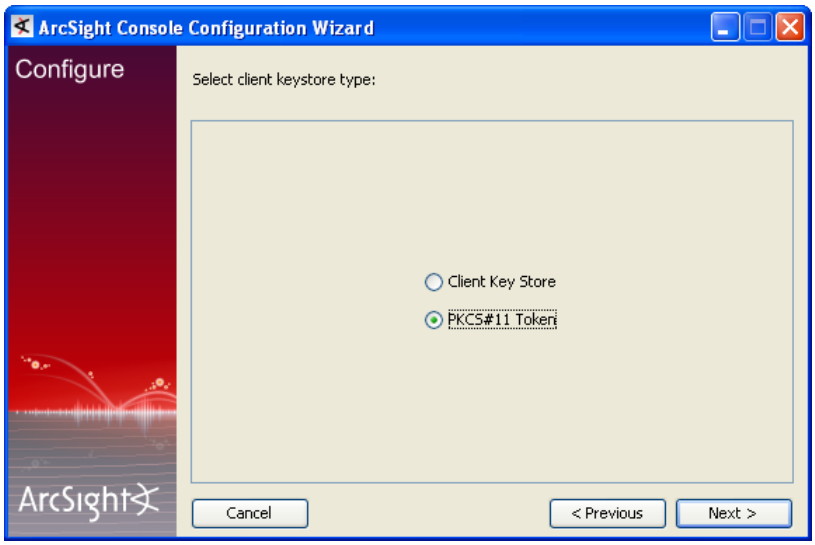
3 Follow the prompts in the wizard screens by accepting all the defaults until you get to the screen for the authentication option shown in the next step.

4 Select the authentication that you selected for the Manager in the following screen.

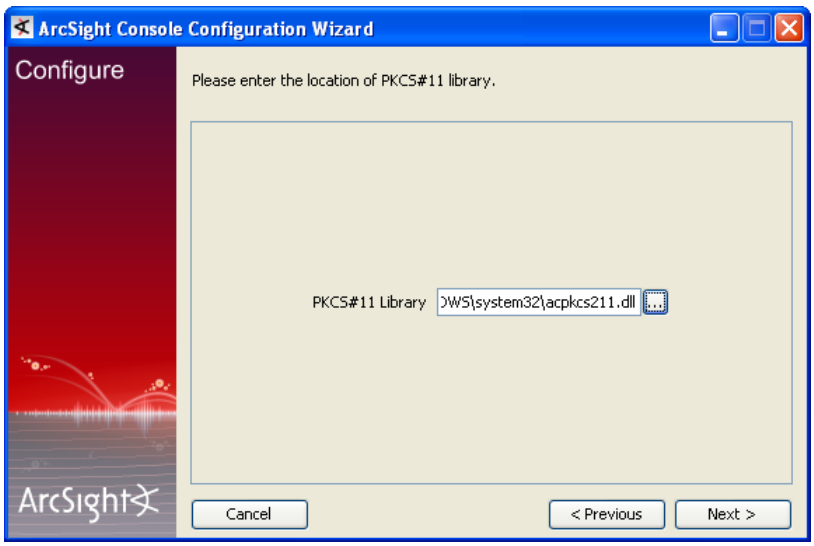


5 Follow the prompts in the next few screens by accepting the defaults.

6 Select **PKCS #11 Token** option in the following screen.



7 Enter the path or browse to the PKCS #11 library as shown in the following screenshot:

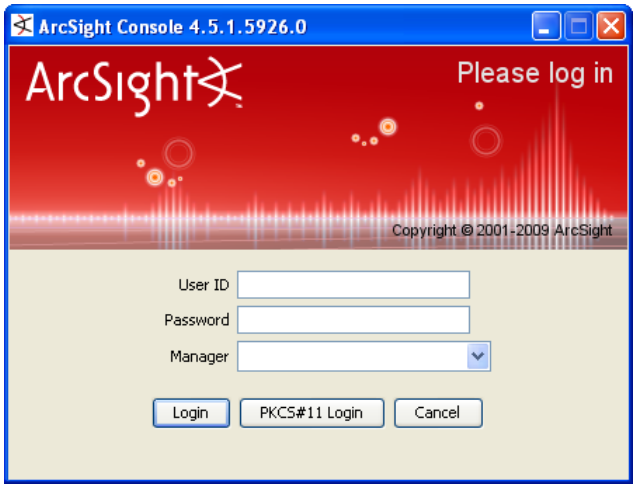


By default, the PKCS #11 library is located in: `C:\windows\system32\acpkcs211.dll`.

8 Complete the setup program by accepting all the defaults.

Logging in to the Console Using CAC

When you start the Console, you will see the following screen:



You have the option to log in using one of the following methods:

- Username and password combination
- PKCS#11 Login

If you selected the PKCS #11 Login option to log in, you will see the following dialog requesting you to enter the PIN number of your ActivClient card. Enter the PIN number for your CAC card in the **PIN** text box.

Appendix D

Restoring Factory Settings

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

Factory reset deletes all event and configuration data

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

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

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

4. Use the mouse or arrow keys to select **System Restore** and press Enter.
5. Click **Acronis True Image Server** to continue.
6. In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press Enter.
7. When the Restore Data Wizard starts, click **Next** to continue.
8. On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.
9. On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.

10 On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** and click **Next**.

11 On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.

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

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

14 On the **Non-empty Destination Hard Disk Drive** page, select **Yes, I want to delete all the partitions on the destination hard drive before restoring** and click **Next**.

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

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

a Select **Validate backup archive for the data restoration process** if you want to validate before resetting the appliance,

Or

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

b Click **Next**.

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

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

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

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

19 If you specified automatic reboot in Step 16, the appliance reboots when the restore is complete. Otherwise, reboot the appliance manually.

20 Follow the instructions and complete the First Boot Wizard. Refer to Chapter 2, Configuring the ArcSight Express v3.0 Appliance, on page 11 for details.

Index