

Installation and Configuration Guide

ArcSight™ ESM Version 4.5 SP2

January 10, 2010



Installation and Configuration Guide ArcSight™ ESM Version 4.5 SP2

Copyright © 2010 ArcSight, Inc. All rights reserved. ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

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

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
01/10/10	ArcSight ESM Version 4.5 SP2	Installation procedures. Separated the FIPS and CAC procedures into their own appendices.

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://support.arcsight.com
Protect 724 Community	https://protect724.arcsight.com

Contents

About this Guide	ix
Related Documentation	ix
Notes, Tips, and Cautions	xi
Text Conventions	xi
Feedback	xii
 Chapter 1: Planning and Installation Overview	 1
What is ArcSight ESM?	1
ArcSight Components	1
ArcSight SmartConnector	2
ArcSight Manager	3
ArcSight Database	3
ArcSight Console	3
ArcSight Web	4
Deployment Overview	6
ArcSight ESM Communication Overview	6
Effect on communication when components fail	7
Deployment Order	8
Supported Platforms	8
Installation Planning	8
Inventory your devices	9
Determine the size and topology of Managers	9
Size your database	9
Event Volume	9
Retention Policy	10
Identify or procure hardware and software	10
Choosing between FIPS Mode or Default Mode	10
Using PKCS#11	11
Import Control Issues	11
Directory Structure for ArcSight Installation	11
Securing your ArcSight ESM System	12
Protecting ArcSight Manager	12
Protecting ArcSight Database	14
ArcSight Built-In Security	15

Physical Security for the Hardware	15
Operating System Security	16
General Guidelines and Policies about Security	17
Deployment Scenarios	18
Scenario 1: A simple, monolithic deployment	18
Scenario 2: A high availability, transparent failover deployment	18
Scenario 3: A hierarchical deployment	20
Scenario 4: A test environment deployment	20
Where to go From Here	21
Chapter 2: Installing ArcSight Database	23
Key Database Installation Success Factors	23
Supported Platforms for Database Installation and Upgrade	24
General Guidelines for Installing Oracle	24
Storage Guidelines	25
Volume 1: SYSTEM Volume	26
Volume 2: DATABASE Volume	26
Volume 3: REDO Volume	28
Volume 4: ARCHIVE Volume	29
Oracle Control Files	30
Selecting an ArcSight Database Template	30
Preparing your Platform for Database Installation	31
UNIX Platforms	31
Preparing a Linux System	32
Preparing a Solaris System	36
Preparing a Windows System	38
Installing or Upgrading ArcSight Database and Oracle	38
Installing the ArcSight Database Software	39
Installing Oracle 10g Database Software	42
Creating a New Oracle 10g Instance	45
Initializing ArcSight Tablespaces, Schema, and Resources	50
Restarting or Reconfiguring ArcSight Database	61
Configuring Partition Management	61
Overview	61
Partition Configuration Parameters	64
Changing Partition Management Configurations	68
Setting Up Partition Archiver	68
Starting and Stopping Partition Archiver	69
Re-registering Partition Archiver with ArcSight Manager	70
Deleting the Partition Archiver Service	70
Reinstalling the Partition Archiver Service	70
Changing the Password for Partition Archiver	71
Uninstalling the ArcSight Database Software	71

Chapter 3: Installing ArcSight Manager	73
ArcSight Manager Supported Platforms	73
Installing the Manager	74
Transferring Configuration from an Existing Installation	76
Selecting the Mode in which to Configure ArcSight Manager	77
Configuring the Manager's Host Name, Port, and Location	77
Java Heap Memory Size	79
SSL Certification Selection	80
Deciding which SSL certificate to select	80
Selecting the SSL certificate	80
Database Connection	83
Authentication	84
How external authentication works	84
Guidelines for setting up external authentication	85
Password Based Authentication	86
Password Based and SSL Client Based Authentication	93
Password Based or SSL Client Based Authentication	93
SSL Client Only Authentication	93
ArcSight Manager Administrator Account Setup	94
Select Packages	94
Mail Server	96
ArcSight Web	99
Asset Auto Creation	100
Setting up as a Service or Daemon	100
Starting and Stopping the Manager	103
Starting the Manager	103
Stopping the Manually Started Manager	103
Running the Manager as a Service	103
Verifying the Manager Installation	103
Reconfiguring ArcSight Manager	104
Securing the ArcSight Manager Properties File	104
Sending Events as SNMP Traps	104
Uninstalling ArcSight Manager	106
Chapter 4: Installing ArcSight Console	109
Console Platforms	109
Using a PKCS#11 Token	110
Installing the Console	111
Transferring Configuration from an Existing Installation	116
Selecting the Mode in which to Configure ArcSight Console	117
Manager Connection	117
SSL Certificate used by Manager	119
Authentication	120

Web Browser	121
User Logs and Preferences	122
Starting the ArcSight Console	124
Logging into the Console	126
Reconnecting to the ArcSight Manager	126
Reconfiguring the ArcSight Console	126
Uninstalling the ArcSight Console	127
Chapter 5: Installing ArcSight Web	129
ArcSight Web Supported Platforms	129
Web Browsers	130
Using a PKCS#11 Token	130
Installing ArcSight Web	131
Setting up SSL Client Authentication	132
Selecting the Mode in which to Configure ArcSight Web	132
Web server Host Name and Port	133
Java Heap Memory Size	134
Enable Case and Events Exports	134
Display Links to Support Web site	135
Is the Manager Configured to use Demo Certificate?	135
ArcSight Manager Host Name and Port	136
Trust Manager Certificate	136
Select Type of Key Pair	137
Authentication	138
Setting ArcSight Web as a Service or Daemon	139
Starting ArcSight Web Manually	140
Connecting to ArcSight Web	141
Styling ArcSight Web	141
Uninstalling ArcSight Web	141
Chapter 6: Installing ArcSight SmartConnectors	143
Deployment Considerations	143
Installing ArcSight SmartConnectors	143
Chapter 7: Establishing Initial ArcSight Resources	145
Defining Zones and Assets	145
Defining Asset Categories	148
Creating Customers and Users	149
Tuning Data Monitors and Rules	150
Appendix A: Configuring an Existing Oracle Installation	151
Creating an ArcSight Instance with an existing Oracle Installation	151
Initializing the ArcSight Schema with an Existing ArcSight Instance	152

Installing Oracle DBMS Without Using the ArcSight Database Installer	152
Appendix B: Using UNCOMPRESSED Archive Type	155
Archiving Uncompressed Files	155
Examples	156
Appendix C: Setting up RADIUS User Authentication	159
Passcodes	159
Defining Shorter ArcSight Internal Login User Names	159
Two-Factor Challenge Responses	160
Steps for Setting Up ACE/Server RADIUS Authentication	161
Installing the ACE/Server and ACE/Server RADIUS Service	161
Configuring the ACE/Server to allow RADIUS Requests	161
Enabling User Accounts in ACE/Server	162
Configuring ArcSight Manager	162
Migrating from Internal Authentication to ACE/Server	163
Authentication Troubleshooting	163
Appendix D: Integrating with iDefense Database	165
Configuring Manager for iDefense	165
Appendix E: ArcSight Manager Failover	167
Architecture	167
Starting Processes	169
Monitoring Processes	169
Next Steps	170
Appendix F: FIPS Compliant State Auditing	171
Compliance State Auditing with Active Channels	171
Compliance State Auditing with Dashboards	172
Compliance State Auditing with Reports	172
Compliance State Auditing with Rules	173
Appendix G: Installing ArcSight ESM in FIPS Mode	175
What is FIPS?	175
Network Security Services Database (NSS DB)	176
What is PKCS?	176
PKCS #11	176
PKCS #12	177
NSS Tools Used to Configure Components in FIPS Mode	177
For More information on NSS Tools	177
TLS Configuration in a Nutshell	177
Understanding Server Side Authentication	178
Understanding Client Side Authentication	179

Setting up Authentication on ArcSight Web - A Special Case	179
Using PKCS #11 Token With a FIPS Mode ESM Setup	180
Installing ArcSight Manager in FIPS mode	180
Setting up Partition Archiver in FIPS Mode	187
Installing ArcSight Console in FIPS mode	189
Connecting a Default Mode Console to a FIPS Enabled Manager	195
Connecting a FIPS Enabled Console to Multiple Managers Running in FIPS 140-2 Mode	196
Installing ArcSight Web in FIPS Mode	196
Configuring Firefox 3.x to Make it FIPS 140-2 Compliant	203
Configuring Internet Explorer to Make it FIPS 140-2 Compliant	206
Installing SmartConnectors in FIPS mode	206
How do I Know Whether My Existing ESM Installation is FIPS Enabled?	206
Migrating an Existing Default Mode ESM Installation to FIPS Mode	207
Manager	207
Console	210
ArcSight Web	212
Appendix H: Using the PKCS#11 Token	217
What is PKCS?	217
PKCS#11	217
PKCS#12	218
PKCS#11 Token Support in ESM	218
An Example - Using the ActivClient CAC Card	218
Using CAC with ArcSight Console	218
Install the CAC Provider's Software	218
Map a User's External ID in the Manager to the CAC's Subject CN	218
Export the CAC's Certificate	220
Extract the Root CA Certificate From the CAC Certificate you Exported	222
Import the CAC Card's Root CA Certificate into the ESM Manager's nssdb	223
Select Authentication Option in Manager Setup	223
Select Authentication Option in Console Setup	224
Logging in to the Console Using CAC	226
Using CAC with ArcSight Web	226
Connecting to ArcSight Web Using CAC	228
Index	231

About this Guide

["Related Documentation" on page ix](#)

["Feedback" on page xii](#)

This section describes the purpose of the ArcSight Installation and Configuration Guide. It also lists other documents available for ArcSight ESM and briefly describes the information contained in those documents.

The ArcSight Installation and Configuration Guide provides you information about ArcSight ESM system components, supported platforms, deployment scenarios, and how to install and configure each component.

Related Documentation

The complete ArcSight documentation set includes guides and Online Help listed in the following table. All guides are available in PDF format.

You can access the guides in these ways:

- From the ArcSight Manager doc directory.
- From the ArcSight Customer Support web site at <https://support.arcsight.com>.
- From the ArcSight Console online Help (click **Help | Browse Arcsight Documentation**).

You can access the ArcSight ESM Online Help from the Help option in ArcSight Console (click **Help | Help Contents**).

Document Title	Description
ESM 101: Concepts for ArcSight™ ESM	ESM 101 introduces the underlying concepts behind how ArcSight ESM works, and provides a roadmap to the tools available in ESM depending on your role in security operations.
ArcSight™ ESM Release Notes	Describes new product features, latest updates, known product issues and work-arounds, and technical support information.
ArcSight™ ESM Installation and Configuration Guide	This Guide.
ArcSight™ ESM Administrator's Guide	Describes how to configure ArcSight and its network interfaces, and maintain ArcSight for ongoing operations.

Document Title	Description
ArcSight™ ESM Reviewer's Guide	Introduces major new features in the current version of ArcSight ESM, including task walk-throughs and usage guidance. The same information is highlighted in the "What's New" Console Help topics.
ArcSight™ ESM User's Guide ArcSight™ ESM Reference Guide	Describes how to use the ArcSight Console. These are printable versions of the online Help topics and glossary.
ArcSight™ ESM Web User's Guide	Provides user and reference information from the ArcSight Web online Help system.
ArcSight™ SmartConnector Configuration Guides	Provides vendor-specific instructions for how to install individual SmartConnectors and configure their associated devices.
ArcSight™ SmartConnector Configuration Guide for ArcSight Forwarding Connector	This guide provides information for installing an ArcSight Forwarding Connector for event collection from an ArcSight ESM Manager installation.
ArcSight FlexConnector Configuration Guide	Describes how to design, create, and install custom SmartConnectors.
ArcSight ESM Upgrade Guides	Provide detailed instructions about how to plan for and execute upgrades from prior releases to the latest version of ESM.
ArcSight™ ESM Release Notes	Describes new product features, latest updates, known product issues and work-arounds, and technical support information.

Notes, Tips, and Cautions



Represents a Note.

Notes provide additional information about a feature or procedure that might help the user make decisions, or inform users about outcomes they can expect.



Represents a Tip.

Tips provide helpful suggestions and best practices about how to get optimum results from a feature or procedure.



Represents a Caution.

Cautions provide information that when ignored may cause system damage, data loss, or bodily injury.

Text Conventions

The following table lists the syntax conventions used in this guide.

Text	Description and Example
Bold	<p>Bold is used to indicate an on-screen element that a user should click. Always use this character format rather than manually bolding the item with the format style menu or “bold” button.</p> <ul style="list-style-type: none"> Enter a value and click OK.
<code>Code</code>	<p>As described before, the code character tag is used for code elements discussed in-line in a paragraph.</p> <ul style="list-style-type: none"> If the name of your active list entries text file is <code>“AdministrativeUsers.txt,”</code> the script would look like this:
<i>Emphasis or BookName</i>	<p><i>Italics</i> indicates emphasis or a book name:</p> <ul style="list-style-type: none"> <i>Do not</i> perform this procedure until you have backed up your data. For more information, see the <i>ArcSight Administrator's Guide</i>.
menu > submenu	<p>Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences.</p> <ul style="list-style-type: none"> menu > submenu > submenu <p>For example:</p> <ul style="list-style-type: none"> Authoring > Rules > Rule Actions > Updating Session Lists
tab subtab	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none"> tab subtab subtab
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none"> All Reports/System Reports/Asset/All Assets

Text	Description and Example
<variable>	<p>A text string enclosed in angular brackets is a variable for which you need to supply a value. (The bracketed text may also be in italics to emphasize that it is a variable.)</p> <p>Example:</p> <p>In <code>--nsp_password=<password></code>, <code><password></code> is a variable for which you supply a value.</p>
{parameter1 parameter2 parameter3}	<p>Curly brackets enclose multiple parameters, at least one of which you must provide.</p> <p>Example:</p> <pre>{--user_id_seq=<user_id> -- user_login=<user_login>}</pre> <p>In the above example, either supply the user ID of a user or his/her login name.</p>
[optional_parameter]	<p>Square brackets enclose parameters, variables, or values that are optional.</p> <p>Example:</p> <pre>[--cli_restrict=1]</pre>

Feedback

To submit feedback regarding ArcSight ESM or documentation, go to ArcSight's customer support web site at <https://support.arcsight.com>

Planning and Installation Overview

This chapter provides a conceptual overview of ArcSight ESM, and offers a high-level description of system components. It helps a network administrator understand planning and deployment issues.

The following topics are covered in this chapter:

["What is ArcSight ESM?" on page 1](#)
["ArcSight Components" on page 1](#)
["Deployment Overview." on page 6](#)
["ArcSight ESM Communication Overview" on page 6](#)
["Deployment Order" on page 8](#)
["Supported Platforms" on page 8](#)
["Installation Planning" on page 8](#)
["Directory Structure for ArcSight Installation" on page 11](#)
["Securing your ArcSight ESM System" on page 12](#)
["Deployment Scenarios" on page 18](#)
["Where to go From Here" on page 21](#)

What is ArcSight ESM?

ArcSight ESM is a Security Information Management (SIM) solution that collects and analyzes security data from heterogeneous devices on your network and provides you a central, real-time view of the security status of all devices of interest to you.

ArcSight ESM components gather and store events generated by the devices you identify. These events are filtered and correlated with events from other devices or collection points to discover risks and assess vulnerabilities.

ArcSight Components

The ArcSight ESM system comprises of the following components, as shown in the following illustration:

- ArcSight SmartConnector
- ArcSight Manager
- ArcSight Database
- ArcSight Console

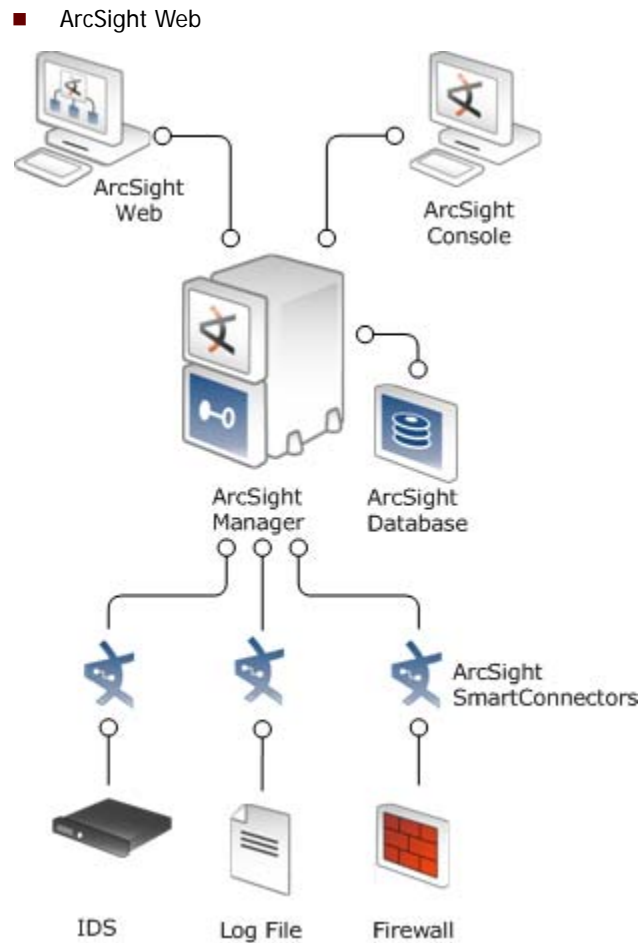


Figure 1-1 ArcSight ESM Components

ArcSight SmartConnector

SmartConnectors (also known as connectors) are the interface for collecting event data from the network devices—such as a firewall, an intrusion prevention system, or a host syslog—that you want to monitor. The connectors gather raw event data comprising of status, alarms, and alerts from these devices. In addition, ArcSight SmartConnectors can also do the following:

- Normalize every alarm and alert into a common security schema
- Filter out unwanted traffic
- Set severity according to a common taxonomy
- Intelligently manage bandwidth to minimize network traffic

SmartConnectors receive event information using SNMP, HTTP, Syslog, proprietary protocols (for example, OPSEC), or direct database connections to the device's repository, such as ODBC or proprietary database connections.

ArcSight SmartConnectors communicate with network devices by either receiving or retrieving information. If the device sends information, the ArcSight SmartConnector receives; if the device does not send information, the ArcSight SmartConnector retrieves from the device.

ArcSight SmartConnectors are available for over 200 network device types found in a typical enterprise infrastructure. For a complete list of available SmartConnectors, see the ArcSight Supported Products (http://www.arcsight.com/product_supported.htm) page.

Depending on the network device a SmartConnector is collecting data from, the connectors can be installed directly on devices (if possible) or separately on connector-dedicated servers.

ArcSight Manager

ArcSight Manager is at the center of the ArcSight ESM solution. The Manager is a server-based system that receives event data from SmartConnectors, processes it to assess and categorize threat levels, and displays information to the ArcSight Console and ArcSight Web. In addition, the ArcSight Manager can send notifications to the devices (such as pagers and cell phones) you specify.

For detailed information about how events received by the Manager are processed, see *ESM 101 Concepts for ArcSight ESM*.

ArcSight Manager can be installed across a variety of operating systems, such as Windows and UNIX, and hardware platforms.

ArcSight Database

ArcSight Database is the central repository for all information collected by the ArcSight Manager. Additionally, the database contains configuration information about the Manager such as users, groups, permissions, rules, assets, and reports.

The database is based on Oracle and is typically installed on a dedicated system separate from the system on which ArcSight Manager is installed.

The database can be installed across a variety of operating systems and hardware platforms. The platform on which the database is installed can be different from the one on which the ArcSight Manager is running.

ArcSight Console

The ArcSight Console is a workstation-based graphical user interface that provides an intuitive interface to perform essential security management tasks. The following graphic shows you an example of the ArcSight Console.

Depending on your job function or need, the Console can be used for a variety of tasks such as:

- Routine monitoring
- Authoring—Setting up filters and creating customized rules, defining notification and escalation procedures, and generating reports
- Administrative tasks—Setting up users and their permissions

- The Console can be installed across a variety of operating systems and hardware platforms.

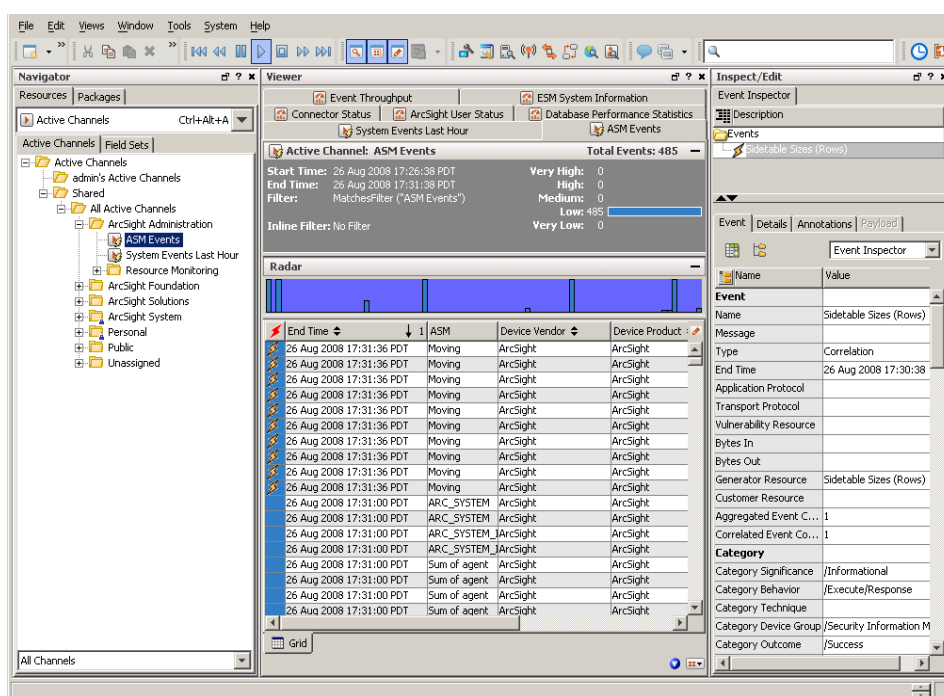


Figure 1-2 Example of ArcSight Console

ArcSight Web

ArcSight Web is a web server that enables you to access ArcSight Manager securely using a browser.

ArcSight Web is intended for users who need to view information on the Manager, but not author or administer it; for example, operators in a Security Operations Center (SOC) and customers of a Managed Security Service Provider (MSSP).

ArcSight Web can be installed on the same server as the ArcSight Manager or on a separate server that has network access to the Manager. If ArcSight Web is installed on a separate server, that server makes secure connections to the Manager on behalf of the browsers requesting data from the Manager.

If the separately installed server is accessible from outside of a protected network, users from outside of that network can use ArcSight Web to access information on the Manager.

The following graphic shows you an example of the ArcSight Web.

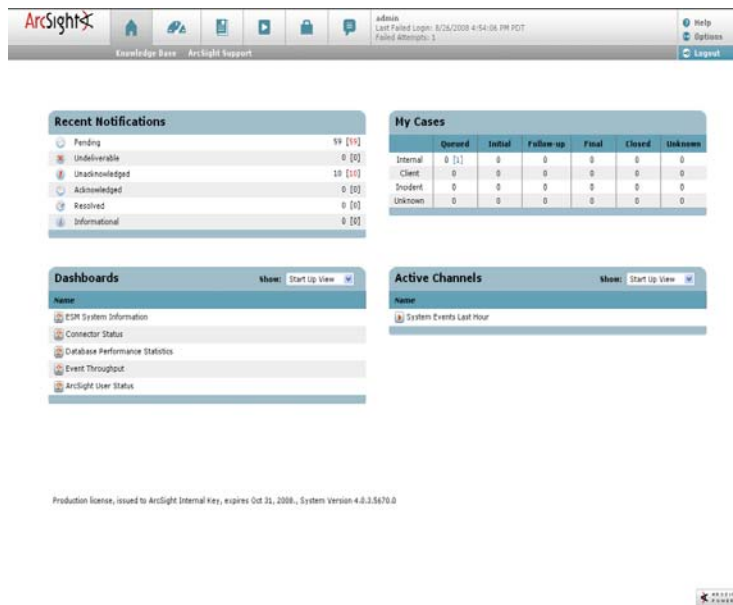


Figure 1-3 Example of ArcSight Web

Deployment Overview.



Make sure that you install both the ArcSight Manager and ArcSight Database on machines that are physically located in the same time zone.

The following is an example of how various ArcSight components can be deployed in a network

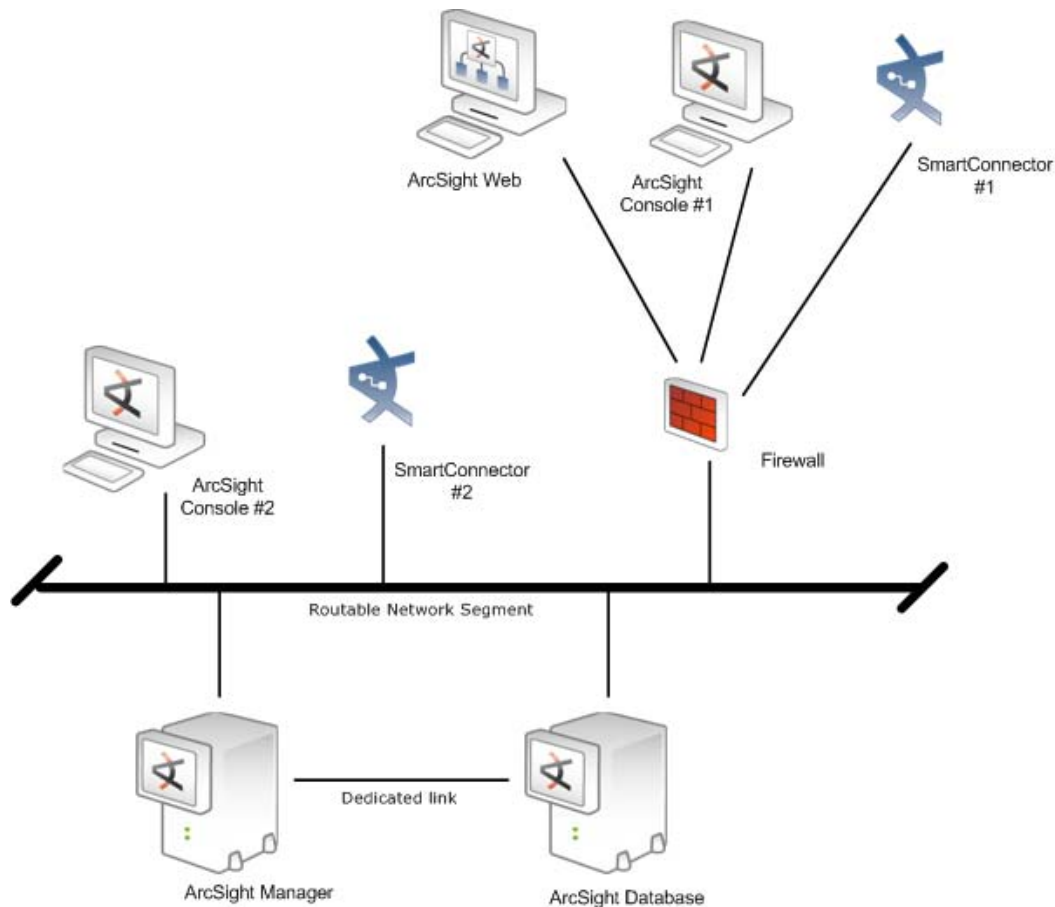


Figure 1-4 ArcSight Components Deployment Overview

There are many other possible topologies such as placing the Manager and the database behind a firewall for an extra layer of protection or installing multiple Managers for redundancy.

Irrespective of the topology you use to deploy SmartConnectors, Consoles, and ArcSight Web, ArcSight strongly recommends deploying the ArcSight Database in close proximity to the Manager, possibly over a dedicated network link with a cross-over cable connection.

ArcSight ESM 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.

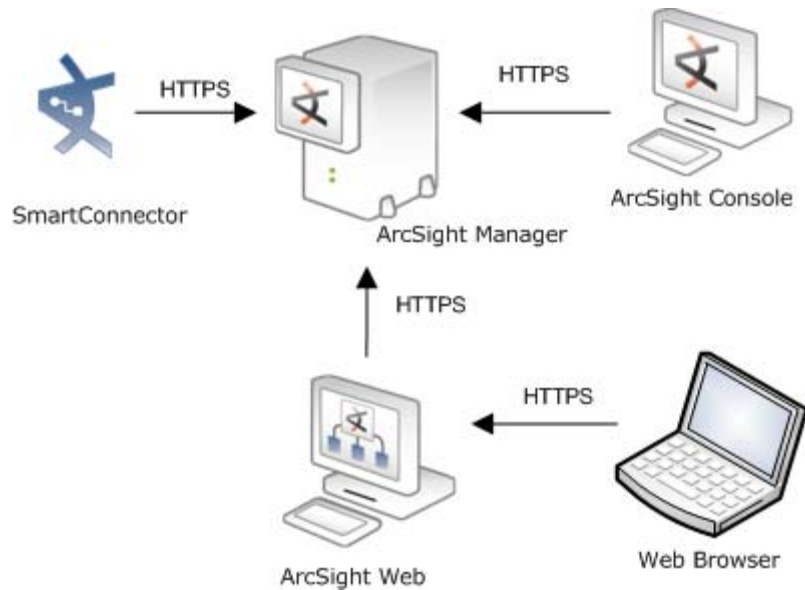


Figure 1-5 ArcSight ESM Communication Overview

SSL works over TCP (Transport Control Protocol) connections. The default incoming TCP port on ArcSight Manager is 8443. For more information on port settings and defaults, see the section on [“Securing your ArcSight ESM System” on page 12](#).

The Manager never makes outgoing connections to the Console, ArcSight Web, or SmartConnectors. However, it does make outgoing connections to the ArcSight Database (the protocol depends on the kind of database), network management solutions (using SNMP), and external authentication solutions via RADIUS and LDAP (if configured). HTTPS is not used between the Manager and the Database.

Effect on communication when components fail

If any of the ArcSight components is unavailable, it can affect communication between other components.

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

If the Manager is unavailable, the SmartConnectors start caching events to prevent event data loss. The TNS listener on the database waits for connections from clients. The database server is idle. The Consoles are 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.

Deployment Order

There are dependencies among the ArcSight components. Therefore, it is important to install the components in this order:

- 1 Database (ArcSight Database)
- 2 Manager
- 3 SmartConnectors or Consoles or Partition Manager (in any order)
- 4 Web Server (ArcSight Web)



Note

Do not deploy the component next in the list until you have ensured that the previous component is completely deployed and functioning as expected.

Supported Platforms



Note

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

All ArcSight ESM system components are software based. You can deploy these components on industry standard heterogeneous platforms, such as UNIX, Windows, Linux, and Macintosh. The components securely communicate with each other over a TCP/IP network using Secure Socket Layer (SSL).

Although multiple components can be installed on single machine, ArcSight strongly recommends against it.

Refer to specific component chapters for details regarding the platform requirements for particular ArcSight components. For supported Web browsers, see the section on [“Installing ArcSight Web” on page 129](#).

Viewing ArcSight reports and product documentation requires Adobe Reader, version 5.0 or later. The Acrobat Reader, which includes a stand-alone program as well as a web browser plug-in, is available at no cost from

<http://www.adobe.com/products/acrobat/readmain.htm>

Installation Planning

Planning involves sizing and determining installation details for each ArcSight component based on your business and network needs.

The first step in planning is to inventory your network to determine the number and type of network devices you want ArcSight to monitor. Typically, device type is directly related to the number of events it will generate on daily basis. For example, firewalls generate a lot of events and a server may not. Once you have determined expected event volume on your network, you can easily size the hardware you will need to collect, process, and store those events.

The next step is to ensure that other elements essential to installation have been procured such as a license, an SSL certificate, and an SMTP server.

The following sections describe these steps on a high level.



ArcSight Professional Services can help create a comprehensive plan for ArcSight deployment and can assist with installation and configuration as well. For more information, contact your ArcSight representative.

Inventory your devices

Inventory your devices and plan the ArcSight SmartConnector that will report on them. The number of SmartConnectors that you can install on a machine depends on the total number of events per second (eps) those connectors will collectively process. Typically, a dual Pentium IV with 2 GB RAM can easily process up to 1500 eps (~130 million events per day), all connectors combined.

Determine the size and topology of Managers

Determine the number and configuration of ArcSight Managers to which the SmartConnectors will report. If you will be using more than one Manager, determine the topology that is most appropriate for your environment. The section at the end of this chapter lists a few common topologies.

Size your database

Use these factors to size your storage requirements:

- Event Volume
- Retention Policy

Event Volume

A raw event is a single “row” or “message” in a log file, a trap, or database of the reporting device. SmartConnectors send these events to the Manager, which stores it in the database. For sizing a database, it is important to know the volume of events that the database will store.

The average size of the data stored for each event depends on the Turbo mode—Fastest, Faster, or Fast—specified for each SmartConnector. In the Fastest mode, a small subset of the event fields from an event is retained. This mode is suited for devices such as firewalls that have relatively less amount of data in an event. Faster mode retains all event fields, without adding additional data. This is the default mode and is adequate for most devices. Fast mode is the most comprehensive turbo mode and includes all event fields available in an event, plus some additional data. Fast mode should be used with care as it has a significant impact on performance.

SmartConnectors can filter raw events to reduce event volume. For example, you can set up your SmartConnector to forward events from a specific network device or specific types of events such as login failures.

Additionally, SmartConnectors can aggregate events with matching values into a single aggregated event. For example, a connector is configured to aggregate events with a specific source and destination address and if the same event occurs within 30 second intervals. If 10 such events occur, the connector aggregates all those events into one single

event, adds an aggregated event count of 10, and forwards it to the Manager. Thus aggregation further reduces event volume.



Note

If both, filtering and aggregation, are configured, event filtering takes place before aggregation.

Retention Policy

Retention period defines the amount of time data is retained in the database. There are three types of retention periods in ArcSight Database:

- Online Uncompressed Partitions (Hot)
- Online Compressed Partitions (Warm)
- Archived Partitions (Cold—on disk archives)

The retention period for online uncompressed partitions specifies the number of days (or latest partitions) for which data will be kept uncompressed. By default, this retention period is set to 2 days. For example, if this retention period is set to 2 and today is April 24th, the data in the partitions created for April 22nd and 23rd will be uncompressed.

The retention period for compressed partitions specifies the number of days (or partitions) for which data will be compressed but kept online. By default, this retention period is set to 28 days. For example, if this retention period is set to 28 and today is April 24th, the data in the partitions created for March 25th through April 21st will be compressed but online.

The retention period for archived partitions specifies the number of days (or partitions) for which data is compressed and archived to a nearline storage device. Any archived partition older than this period is purged and cannot be reactivated easily. By default, this retention period is set to 60 days. For example, if this retention period is set to 60 and today is April 24th, the data in partitions created for Jan 24th through March 24th will be compressed and archived to a specified nearline storage device.

Identify or procure hardware and software

Based on the data you collect in previous steps, choose appropriate hardware and software platforms based on supported platforms that are listed in the specific component chapters.

Choosing between FIPS Mode or Default Mode



Caution

Not all ESM versions or ArcSight Express models support the FIPS mode.

Starting in ESM v4.0 SP2, ArcSight ESM supports the Federal Information Processing Standard 140-2(FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet these standards.

You can now choose to install the ESM components in the FIPS mode if you have the requirements to do so.

Using PKCS#11



PKCS#11 token support may not be available for all ESM versions and ArcSight Express models.

Starting in ESM v4.0 SP2, ArcSight ESM supports the use of a PKCS#11 token such as the Common Access Card (CAC) to log into the Console or ArcSight Web. PKCS#11 is Public-Key Cryptography Standard (PKCS), published by RSA Laboratories which describes it as “a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.”

You can use the PKCS#11 token to log in regardless of the mode in which ArcSight Console or ArcSight Web is running - in FIPS 140-2 mode or default mode.

Import Control Issues

If you are a customer in the United States, you can skip reading this section. If you are a customer outside of the United States, you need to be aware of your country's restrictions on allowed cryptographic strengths. The embedded JRE in ArcSight components, ship with the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files and they are enabled by default. These files are:

- `jre\lib\security\local_policy.jar`
- `jre\lib\security\US_export_policy.jar`

This is appropriate for most countries. However, if your government mandates restrictions, you should backup the above two *.jar files and use the restricted version files instead. They are available at:

`jre\lib\security\local_policy.jar.original`

`jre\lib\security\US_export_policy.jar.original`

You will have to rename *.jar.original to *.jar.

The only impact of using the restricted version files would be that you will not be able to use ArcSight's keytoolgui to import unrestricted strength key pairs. Also, you will not be able to save the keystore if you use passwords that are longer than four characters. No other ESM functionality is impacted.

Directory Structure for ArcSight Installation

ArcSight ESM software components install consistently across UNIX and Windows platforms. Whether a host is dedicated to the ArcSight Database, Manager, Console or other component, by default, ArcSight software is installed in a directory tree under a single root directory on each host. (DBMS and other third-party software is not necessarily installed under this directory, however.) The path to this root directory is called `<ARCSIGHT_HOME>`.

Typical examples of `<ARCSIGHT_HOME>` include `/usr/arcsight/manager` on a UNIX system, or `C:\arcsight\Manager` on a Windows system.

The directory structure below `<ARCSIGHT_HOME>` is also standardized across components and platforms. The following table lists a few of the commonly used directories across the components.

Port	Directory
ArcSight ESM Software	<code><ARCSIGHT_HOME>\bin</code>
Properties files	<code><ARCSIGHT_HOME>\config</code>
Log files	<code><ARCSIGHT_HOME>\logs</code>

Securing your ArcSight ESM System

Follow the information in the following sections to protect your ArcSight component.



By default, the minimum length for passwords is six characters and the maximum length is 20 characters.

Protecting ArcSight Manager

Never run ArcSight Manager as root.

Don't use demo SSL certificates in production. Make sure when switching that you remove the demo CA from cacerts on all SmartConnectors and Consoles.

Closely control access to files, using the principle of least privilege, which states that a user should be given only those privileges that the user needs to complete his or her tasks. The following files are particularly sensitive:

- `<ARCSIGHT_HOME>\config\jetty\keystore` (to prevent the ArcSight Manager private key from being stolen)
- `<ARCSIGHT_HOME>\config\jetty\truststore` (w/ SSL Client authentication only, to prevent injection of new trusted CAs)
- `<ARCSIGHT_HOME>\config\server.properties` (has keystore and database passwords)
- `<ARCSIGHT_HOME>\config\jaas.config` (w/ RADIUS or SecurID enabled only, has shared node secret)
- `<ARCSIGHT_HOME>\config\client.properties` (w/ SSL Client authentication only, has keystore passwords)
- `<ARCSIGHT_HOME>\reports\sree.properties` (to protect the report license)
- `<ARCSIGHT_HOME>\reports\archive*` (to prevent archived reports from being stolen)
- `<ARCSIGHT_HOME>\jre\lib\security\cacerts` (to prevent injection of new trusted CAs)
- `<ARCSIGHT_HOME>\lib*` (to prevent injection of malicious code)
- `<ARCSIGHT_HOME>\rules\classes*` (to prevent code injection)

Use a host-based firewall. On the ArcSight Manager, block everything except for the following ports. Make sure you restrict the remote IP addresses that may connect to those that actually need to talk.

Port	Flow	Description
22/TCP	Inbound	SSH log in (Unix only)
53/UDP	Inbound/Outbound	DNS requests and responses
8443/TCP	Inbound	SmartConnectors and Consoles
1521/TCP	Outbound	Oracle
25/TCP	Outbound	SMTP to mail server
110/TCP	Outbound	POP3 to mail server, if applicable
143/TCP	Outbound	IMAP to mail server, if applicable
1645/UDP	Inbound/Outbound	RADIUS, if applicable
1812/UDP	Inbound/Outbound	RADIUS, if applicable
389/TCP	Outbound	LDAP to LDAP server, if applicable
636/TCP	Outbound	LDAP over SSL to LDAP server, if applicable

Block all inbound ports on the ArcSight database except the following:

Port	Flow	Description
22/TCP	Inbound	SSH log in (Unix only)
53/UDP	Inbound/Outbound	DNS requests and responses
1521/TCP	Inbound	Oracle



If your database is set up on Microsoft Windows platform and you have blocked inbound ports as described above, your connections to the database might fail.

This behavior is observed because Oracle database, running on Windows, redirects connection requests coming from its clients on port 1521 to different, non-standard ports. When the client tries to establish a connection on the redirected port, it is blocked by the firewall. For more information, see the OracleMetaLink bulletin Solving Firewall Problems on Windows (Doc ID: Note:68652.1) at <https://metalink.oracle.com/>.

To allow successful connections in such a setup, you need to open all inbound TCP ports between your Manager and your database IP addresses or use SQL*Net proxy for your firewall.

As another layer of defense (or if no host-based firewall is available), you can also restrict which connections are accepted by the ArcSight Manager using the following properties in the server.properties file:

`web.accept.ips=`

`xmlrpc.accept.ips=`

```
agents.accept.ips=
```

Each of these properties takes a list of IP addresses or subnet specifications, separated by commas or spaces. Once specified, only connections originating from those addresses are accepted. The `xmlrpc.accept.ips` property restricts access for ArcSight Consoles and the ArcSight Web server. The `agents.accept.ips` property restricts access for SmartConnectors. For registration, the SmartConnectors need to be in `xmlrpc.accept.ips` as well, so that they can be registered. The format for specifying subnets is quite flexible, as shown in the following example:

```
web.accept.ips=192.168.10.0/24 192.168.30.171
```

```
xmlrpc.accept.ips=192.168.10.120 192.168.10.132
```

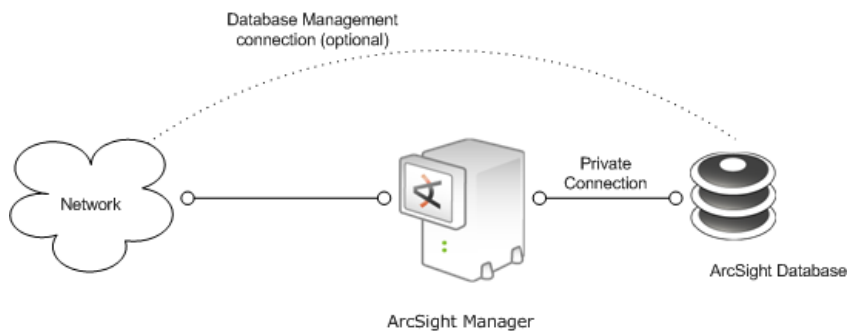
```
agents.accept.ips=10.*.*.*,192.168.0.0/255.255.0.0
```

Protecting ArcSight Database

Secure the link between the ArcSight Manager and Oracle as the Oracle protocol transmits the Oracle password as well as event data and other sensitive data in clear. The options described here include a private network (preferred) or a tunnel (if performance is less important).

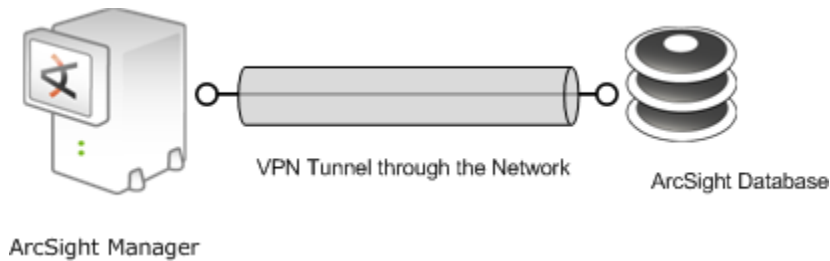
You can secure the communication path between ArcSight Database and ArcSight Manager in these ways:

- Dedicated (private) connection between the Manager and the database



Run a dedicated network between ArcSight Manager and ArcSight Database. Use a second network interface for the Manager host machine and connect it to a dedicated network in which only the database host machine is present (that is, using a dedicated switch/HUB or a crossover Ethernet cable to connect the hosts). While this approach provides the best performance, it might be difficult to achieve in some environments due to logistic constraints. In most cases, it is required to access the database host machine from the public network in order to manage it. So, it is recommended to use a second interface on the database host machine in order to connect it to the main network.

- Use a Virtual Private Network (VPN) tunnel between the Manager and Database



In this scenario, the communication between the database and the Manager is encrypted before it is sent over. ArcSight recommends using IPSec VPNs or SSH (Secure Shell) tunnels.

The advantage of using VPNs is that they enable secure communication over public networks. However, the overhead of encrypting and decrypting data can impact performance.

If you are deploying on a storage area network (SAN), use access control lists to prevent other hosts on the SAN from accessing volumes that contain ArcSight Database files. Equivalently, you can configure the TNS listener on the Oracle side to restrict source IP addresses.

ArcSight Built-In Security

ArcSight user accounts have user types that control the functions which users can access in the ArcSight Manager. The "Normal User" type has the most privileges. Where possible, use more restrictive types, such as "Manager SmartConnector," "Management Tool," or "Archive Utility" for non-human user accounts. This is particularly important when user passwords must be stored in scripts for unattended execution.

Apply the principle of least privilege when creating user accounts in ArcSight and when granting access to resources or events. Users should not have more privileges than their tasks require.

Physical Security for the Hardware

In addition to establishing security policies for passwords, keystores, and other software facilities, it is important to provide physical security for the hardware used by the ArcSight ESM system. Physical hardware includes computers running ArcSight Console, Manager, Database, and SmartConnector software, as well as the network which connects them.

Physical access to computers running ArcSight software must be restricted. Windows computers that run ArcSight software require network domain passwords to authenticate

users, because the operating system may cache passwords used for logging into ArcSight components.

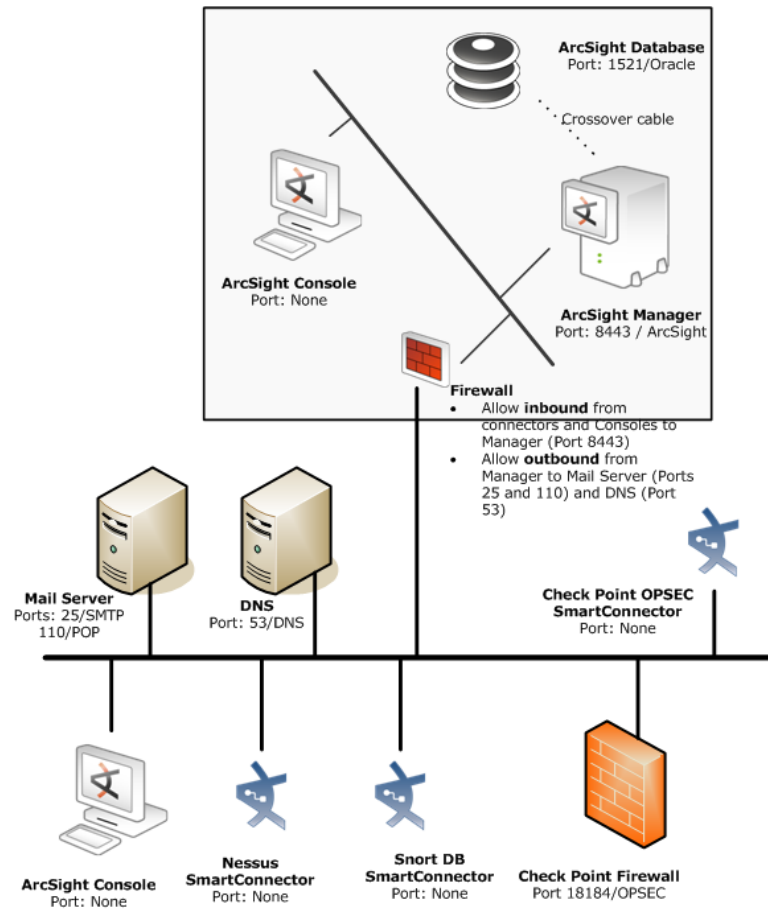


Figure 1-6 Physical security for hardware

Typical ArcSight deployment, illustrating the technique of deploying ArcSight Manager and Database behind a firewall. The ports listed in the above graphic are open ports on the device for server connections.

- Use the locking mechanisms provided by most rackmount cases to prevent malicious/accidental tampering with the machine.
- Use locks on disk drive enclosures.
- Use redundant power and uninterruptible power supplies (UPS).
- Protect the BIOS (x86 systems only) or firmware (IBM and Sun systems):
 - ◆ Disable all floppy and CD-ROM drives for booting so that the system can only be booted from the hard disk.
 - ◆ Disable COM, parallel, and USB ports so that they can't be used to extract data.
 - ◆ Disable power management.

Operating System Security

- On Linux, set up a boot loader password to prevent unauthorized people from booting into single user mode (see the LILO or GRUB documentation for details).

- On Linux, disable reboot by Ctrl-Alt-Del in `/etc/inittab`. Comment out the line that refers to “ctrlaltdel.”
- Set up a screen saver that prompts for a password with a moderately short delay (such as five minutes).
- Disable power management in the OS.
- When installing the OS, select packages individually. Only install what you know will be needed. You can always install missing packages as you encounter them.
- Run automated update tools to obtain all security fixes. Visit <http://windowsupdate.microsoft.com> for Windows systems and run the Microsoft Security Baseline analyzer to get missing patches. Use up2date on Red Hat Linux (may require Red Hat Network subscription). For Solaris, check <http://sunsolve.sun.com>.
- Uninstall (or at least turn off) all services that you don't need. In particular: finger, r-services, telnet, ftp, httpd, linuxconf (on Linux), Remote Administration Services and IIS Services on Windows.
- On Unix machines, disallow remote root logins (for OpenSSH, this can be done using the `PermitRootLogin` no directive in `/etc/ssh/sshd_config`). This will force remote users to log in as a non-root user and `su` to root, thus requiring knowledge of two passwords to gain root access to the system. Restrict access to `su`, using a “wheel group” pluggable authentication module (PAM) so that only one non-root user on the machine can `su` to root. Make that user different from the arcsight user. That way, even if the root password is known and an attacker gains access through ArcSight in some way, they won't be able to log in as root.
- Rename the Administrator/root account to make brute force attacks harder.

General Guidelines and Policies about Security

Educate system users about “social engineering” tricks used to discover user account information. No employee of ArcSight will ever request a user's password. When ArcSight representatives are on site, the administrator of the system will be asked to enter the password and, if needed, to temporarily change the password for the ArcSight team to work effectively.

Educate users to use secure means of communication—such as SSL to upload to `software.arcsight.com` or PGP for e-mail—when transferring configuration information or log files to ArcSight.

Set up a login banner stating the legal policies for use of the system and the consequences of misuse. (Instructions for creating a login banner vary by platform.) ArcSight Consoles can also display a custom login banner. Contact ArcSight Customer Support for more information.

Choose secure passwords. (No password used in two places, seemingly random character sequences, eight characters or longer, containing numbers and special (non-letter) characters). Passwords are used in the following places—if any one is breached, the system is compromised:

- All database accounts (arcsight, SYS, SYSTEM)
- The arcsight user and root user on the system that runs the Manager
- The oracle user and root user on the system that runs the Database
- All users created in ArcSight
- The SSL keystores
- The boot loader (Linux)

- The BIOS (x86 systems only)
- The RADIUS node secret
- The LDAP password for ArcSight Manager (w/ basic authentication only), where applicable

Consider purchasing and using a PKI solution to enable SSL client authentication on Consoles and SmartConnectors.

Consider purchasing and using a two-factor authentication solution such as RSA SecurID.

Make sure that all the servers with which ArcSight interacts (DNS, Mail, RADIUS, etc.) are hardened equivalently.

Use a firewall and intrusion detection systems to secure the network that runs the ArcSight Manager and ArcSight Database.

Deployment Scenarios

You can deploy ArcSight ESM in a number of ways depending on your business needs and budget. The following are a few recommended scenarios.

You can mix the deployment principles described for one scenario with another. For example, you can implement a distributed deployment (Scenario 3) in which the lower-level managers are standalone systems (as described in Scenario 1) but the top-level manager is implemented in a transparent failover configuration (Scenario 2).

Scenario 1: A simple, monolithic deployment

As shown in the illustration below, in a simple deployment an ArcSight Manager, ArcSight Database, and SmartConnectors are installed on three distinct systems. In this example, the three SmartConnectors are installed on distinct systems as well; however, you can have the three SmartConnectors installed on a single system (if the total event per second from the three SmartConnectors does not exceed the recommended value).

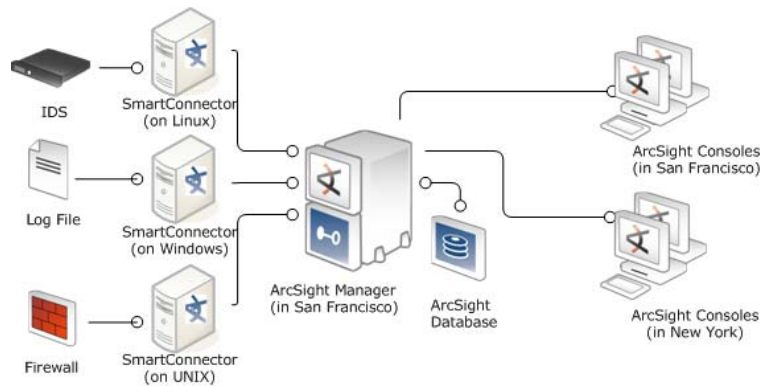


Figure 1-7 A Simple, Monolithic Deployment

Scenario 2: A high availability, transparent failover deployment

As shown in the illustration below, you can set up two ArcSight Managers in a failover group using a third-party Failover Management (FM) software solution. One of the Managers in this group is active, while the other one is on standby. If the FM software

detects that the ArcSight Manager service is not running on the active Manager, it tries to restart the service. If the service restart fails, the FM software shuts down the service on the active Manager and brings it up on the standby Manager.

Clients—SmartConnectors, ArcSight Console, ArcSight Web—connect to the virtual IP address that the FM software assigns to the failover group. Therefore, when the standby Manager becomes active, the clients continue to connect to the same IP address as before although the physical system they are connecting to is different.

In addition to the Managers, the database servers are also set up using a database-specific FM software. The active ArcSight Manager connects to the virtual IP address of the failover group of the database servers. All database files and the Manager directory to which the active Manager frequently writes its state must be on shared storage so that they are available to the active and standby systems at any time.

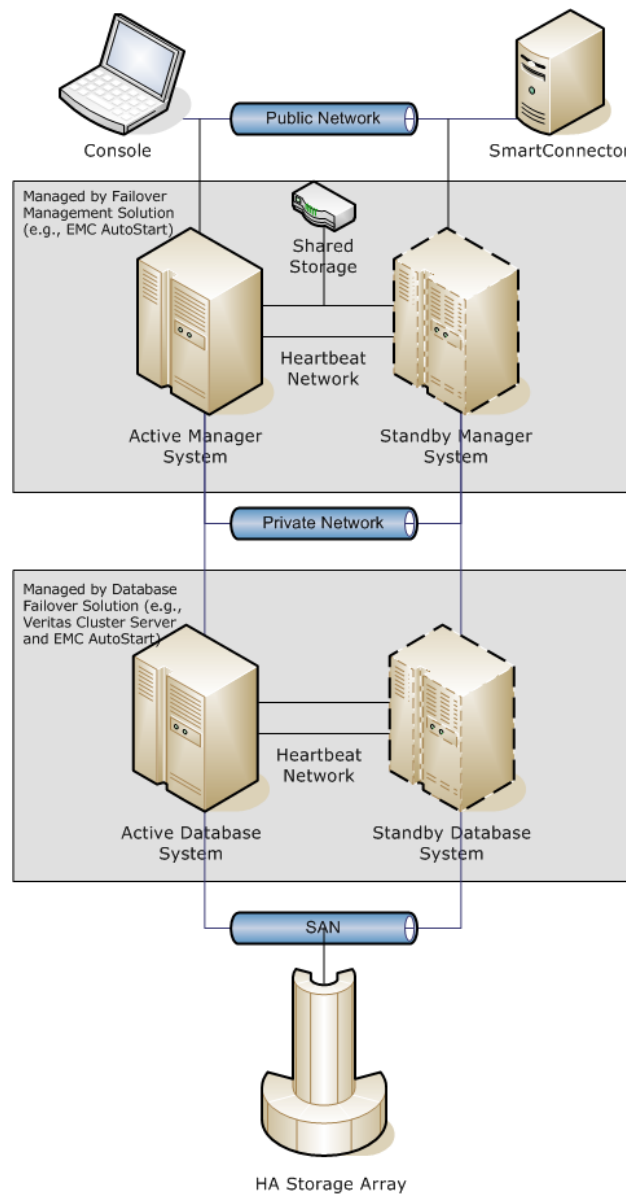


Figure 1-8 A High Availability, Transparent Failover Deployment

Scenario 3: A hierarchical deployment

As shown in the illustration below, you can deploy ArcSight Managers such that data from lower-level Managers is forwarded to a central, top-level Manager. This type of deployment works well for organizations that want to set up Managers according to organizational units, organizations with geographically dispersed locations, and MSSPs.

The lower-level managers collect and process events from their local SmartConnectors. In addition, these Managers forward key events to the central Manager thus enabling the central Manager to provide a holistic view of the security status of the entire network.

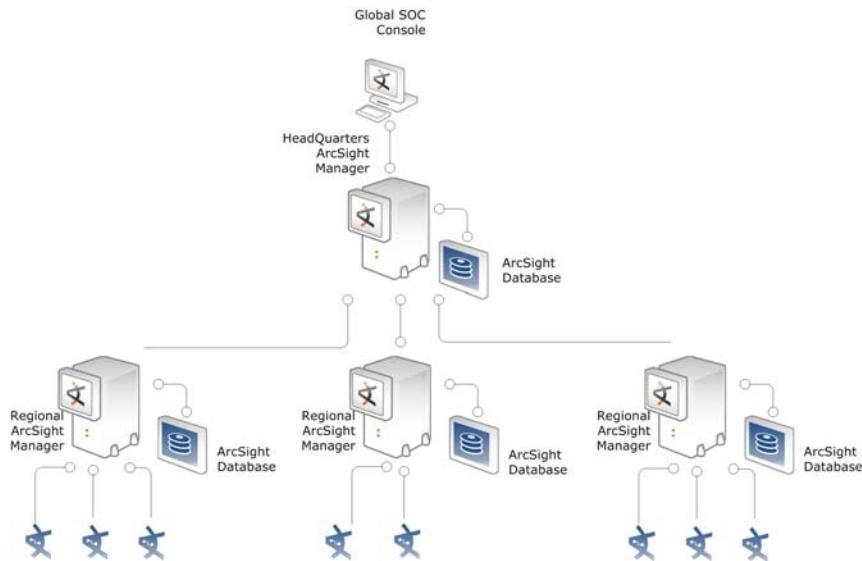


Figure 1-9 A Hierarchical Deployment

Scenario 4: A test environment deployment

As shown in the illustration below, you can set up your production SmartConnectors to forward events to two ArcSight Managers--to a production Manager and to a separate ArcSight Manager running in a test environment. By doing so, you can test rules, filters, or

any other changes on your test environment Manager before implementing them in your production environment.

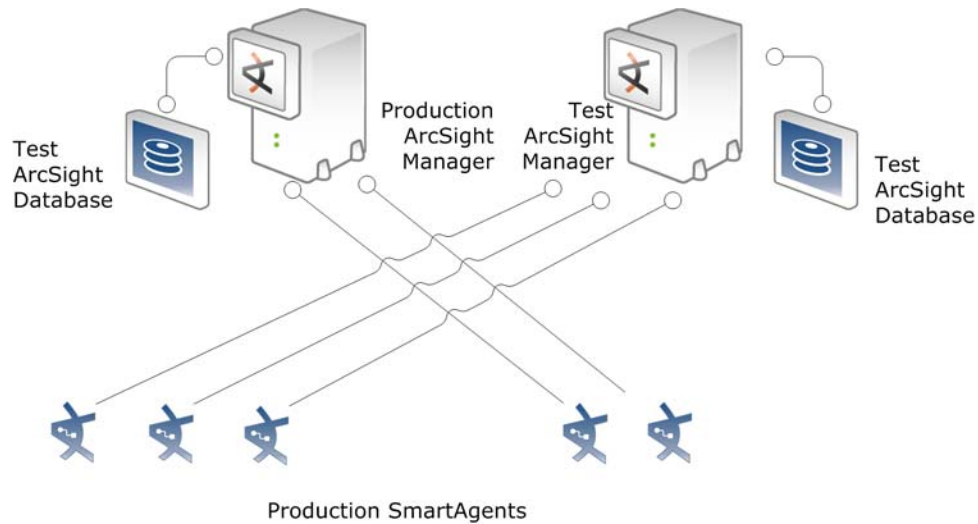


Figure 1-10 A Test Environment Deployment

Where to go From Here

Here are the steps you will use to install and configure ArcSight:

DBMS and ArcSight Database Installation. ArcSight Database installation installs Oracle DBMS Enterprise Edition with partitioning support. Once the DBMS is installed, you configure the database and partition policies. You can also use your existing Oracle installation.

ArcSight Manager Installation. Once the DBMS has been established, you will install the ArcSight Manager, establish initial users, and configure options such as e-mail notification.

ArcSight Console Installation. Install and configure the ArcSight Console, then start ArcSight Manager and run the ArcSight Console to confirm successful installation. The ArcSight Console also provides more visibility when you install Connectors, which you will do in the next and final installation step.

ArcSight SmartConnectors Installation. Install SmartConnectors on a preferably dedicated UNIX or Windows machine.

ArcSight Web Installation. ArcSight Web is a standalone web server that interacts with the Manager and can operate outside a firewall that protects the Manager. Thus users can use supported browsers to access information from the Manager. You can install ArcSight Web on the same host as the ArcSight Manager or on a separate machine that has network access to the Manager.

Chapter 2

Installing ArcSight Database

The first step in the process of installing the ArcSight system is installing and configuring the ArcSight database and its underlying database management system.

The following topics are covered in this chapter:

- ["Key Database Installation Success Factors" on page 23](#)
- ["Supported Platforms for Database Installation and Upgrade" on page 24](#)
- ["General Guidelines for Installing Oracle" on page 24](#)
- ["Preparing your Platform for Database Installation" on page 31](#)
- ["Installing or Upgrading ArcSight Database and Oracle" on page 38](#)
- ["Restarting or Reconfiguring ArcSight Database" on page 61](#)
- ["Configuring Partition Management" on page 61](#)
- ["Uninstalling the ArcSight Database Software" on page 71](#)

The ArcSight Database Installer installs Oracle Database Management System (DBMS) and the ArcSight Database software. However, if you are planning to use an existing Oracle installation, see [Appendix A, Configuring an Existing Oracle Installation, on page 151](#).



Not all ESM versions or ArcSight Express models support the Partition Archiver.

Key Database Installation Success Factors

- Carefully plan your database deployment based on your performance and data retention requirements. Follow platform-specific configuration instructions and prepare data volumes as described.
- Set up e-mail notification when you install the Manager. The ArcSight configuration wizard makes this a simple process, requiring only that an SMTP server be addressable from the Manager host.
- Do not ignore e-mail messages about ArcSight Database from the ArcSight Manager. Messages with WARNING or ERROR on the subject line indicate that the database could stop accepting security events in the near future.

Customizing any aspect of the underlying DBMS, beyond what is described in this chapter, may cause malfunction of ArcSight components. ArcSight Database is only tested and certified using the DBMS configuration described here. If you must customize the DBMS, deploy changes provisionally and monitor ArcSight logs closely.

Supported Platforms for Database Installation and Upgrade

ArcSight recommends installing Oracle 10g. The following operating system platforms and database versions are supported.

Operating System	Database	Typical System Configuration
Windows Server 2003 R2 SP2 (32-bit and 64-bit)	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Red Hat Enterprise Linux 4.0 AS (RHEL 4 AS), update 8 (32-bit and 64-bit)	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Red Hat Enterprise Linux 5.0 AS (RHEL 5.2 AS), update 2 (32-bit and 64-bit)		
SUSE Linux 10 SP2 Enterprise Server (64-bit)		
Sun Solaris 10 (64-bit)	Oracle 10.2.0.4	Sparc-compatible multi-CPU system with 2-16 GB RAM
IBM AIX 5L, Version 5.3 (5.3.0.70) (64-bit)	Oracle 10.2.0.4	Power PC multi-CPU system with 2-16 GB RAM, 2 GB disk space

+ See [“Uninstalling the ArcSight Database Software” on page 71](#) for additional steps you must perform if you apply an Oracle patch or patch set to this configuration.



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

General Guidelines for Installing Oracle

Below are some of the guidelines for installing the Oracle software:

Storage Guidelines

The following table lists typical disk space requirements for installing Oracle10g:

Space type	Amount of space required
Temporary Space	<code>\$TEMP</code> or <code>\$TMPDIR</code> (/tmp, by default) on Unix and <code>%TEMP%</code> on Windows. Must have at least 65 MB available.
Unix Swap Space	(Unix only) Oracle recommends a minimum of two times physical memory for swap space. The ArcSight Database Installer enforces this recommendation if physical memory is less than 4 GB. On machines with more than 4 GB, the installer requires a minimum swap space equal to physical memory size.
Oracle Installation	At least 4 GB in the Oracle installation directory.
ArcSight Database Software	At least 1 GB in the ArcSight Database installation directory.

ArcSight recommends that you use the Stripe and Mirror Everything (SAME) layout for efficiency and space economy, and define volumes as listed below. SAME simplifies sizing and management of a volume without impacting performance. In addition, Oracle recommends using SAME for its databases.

Volume Name	Contents	Typical Size	I/O Load
SYSTEM	Oracle installation	2 GB	Moderate
DATABASE	Oracle default tablespaces and ArcSight tablespaces	Hundreds of GB	High
REDO	Oracle redo log files	10-20 GB	Highest
ARCHIVE	Archived Oracle redo log files and ArcSight partition archives (if Partition Archiver is enabled)	Up to hundreds of GB	Low



Caution

- Typically, the Oracle software is installed on the same drive where the system operating system is installed and user home directories reside. It is not necessary to have a separate volume for Oracle installation.
- You must always create a separate REDO volume to hold redo logs. Do not use the DATABASE volume for this purpose. Additionally, always place the active redo logs on a separate volume from the one used for archived redo logs. ArcSight does not recommend using the same shared volume for redo logs and archived redo logs as it can impact performance.

ArcSight recommends RAID level 1+0 and level 0+1, in order of preference, due to its combination of performance and reliability and does not support RAID 5 for the ArcSight Database.

Volume 1: SYSTEM Volume

Oracle installation directory

The SYSTEM volume stores the Oracle installation. The Oracle installation directory contains Oracle DBMS software. ArcSight recommends that you install Oracle in the default location whenever possible: `/home/oracle` on Unix or Linux, or `C:\oracle` on Windows.

Before installing Oracle, ensure that the Oracle installation directory has adequate available space.

On Unix or Linux, Oracle's Universal Installer, which is invoked in silent mode by ArcSight's Database Installer, cannot check available disk space if you use a symbolic link to the installation directory.

The initial Oracle installation directory size in the previous table includes:

Size	For...
2 GB	Oracle10g installation files
2 GB	ArcSight Database Installer staging space for uncompressed Oracle installation files. The ArcSight Installer extracts the contents of the compressed installation files into the stage subdirectory. The Installer will delete the stage subdirectory when the installation is complete.

Data redundancy is essential for production setups, as loss of information in the SYSTEM volume can leave the database in a state that would require time-consuming recovery. Consequently, a RAID1 (mirroring) configuration is recommended.

ArcSight Database Software

Install the ArcSight Database software in its default location (`/usr/local/arcsight/db` on Unix or Linux, or `C:\arcsight\db` on Windows). Before installing a new version, rename the existing directory by adding the old version number to the directory name.

Volume 2: DATABASE Volume

The DATABASE volume holds these tablespaces:

Oracle's default tablespaces:

- SYSTEM
- SYSAUX (for 10g)
- INDX
- UNDOTBS1
- TEMP

ArcSight tablespaces:

- ARC_SYSTEM_DATA
- ARC_SYSTEM_INDEX

- ARC_EVENT_DATA
- ARC_EVENT_INDEX
- ARC_UNDO
- ARC_TEMP



By default, the Oracle default tablespaces are in the Oracle software installation directory. If the Oracle software installation directory is not mirrored, you must put them on the DATABASE volume.

Due to size and I/O load, NAS (Network Attached Storage) or SAN (Storage Area Network) technology is typically used for the DATABASE volume.

Even though NAS is supported, you have to be aware that the database is very I/O intensive. So, replacing the dedicated connection with a shared network layer could lead to performance issues.

SYSTEM

The SYSTEM tablespace holds all tables of the Oracle data dictionary.

SYSAUX

The SYSAUX tablespace is an auxiliary tablespace to SYSTEM. Many database components use the SYSAUX tablespace as the default location to store data.



The database instance created by the ArcSight's embedded Oracle installer (ArcSight Database installer) has the SYSTEM and SYSAUX tablespaces set to autoextend. These tablespaces will grow in the initial few days after installation as the event collection ramps up. They will stabilize subsequently in terms of size. However, the size of these tablespaces will continue to be a small fraction of the space used by ARC_EVENT_DATA tablespace. If you installed Oracle without using ArcSight's embedded Oracle installer, ensure that you have turned autoextend on for SYSTEM and SYSAUX tablespaces.

INDX

This tablespace holds the indices on the tables of the Oracle data dictionary.

UNDOTBS1

This is Oracle's default UNDO tablespace. An undo tablespace is used to hold the old image to enable a roll back of a transaction and to provide a consistent image to queries that are run after a transaction is initiated but before it is committed. This volume has random read/write I/O.

TEMP

The TEMP tablespace is the default temporary tablespace for the instance and is created during instance creation. This tablespace is used by Oracle's administrative accounts—SYS and SYSTEM. ArcSight schema owner uses another temporary tablespace called ARC_TEMP, which is created during ArcSight Database initialization.

ARC_SYSTEM_DATA

ARC_SYSTEM_DATA stores ArcSight resources such as system objects. Unless very large active lists or large number of assets are used, the space requirements for ARC_SYSTEM_DATA are rather moderate; typically, a few GB.

I/O usage on ARC_SYSTEM_DATA is rather moderate in comparison with ARC_EVENT_DATA, since it is mostly human-driven, and ArcSight Manager memory caches reduce the number of queries substantially.

ARC_SYSTEM_INDEX

ARC_SYSTEM_INDEX holds indexes that enable efficient queries against the data in ARC_SYSTEM_DATA. The I/O load on this tablespace is moderate. ArcSight Manager caches data from ARC_SYSTEM_DATA.

ARC_EVENT_DATA

The ArcSight event data tablespace (ARC_EVENT_DATA) stores all events that are online and accessible from the ArcSight Console. Therefore, this tablespace typically has a very large number of I/O operations, both reads and writes. Writes are caused by inserting new events, as well as by event annotations caused by users or rules. Even though the majority of writes are append operations, the majority of I/O operations on this volume use random access. Write pauses are rare, due to the constant incoming stream of events.

Read operations take place at the same time. These are driven by active channels engaged in the ArcSight Console and ArcSight Web, and by reports and other components of the ArcSight Manager that need to read events. Read operations are mostly random, depending on the various queries. Certain operations, such as running a report, can cause spikes in read I/O, but active channels typically provide a solid base load, depending on filter complexities and time ranges.

ARC_EVENT_INDEX

ARC_EVENT_INDEX is the largest tablespace and holds indices that enable very efficient queries against the data in ARC_EVENT_DATA. Typically, the indices use more disk space than the actual data.

Again, most I/O load occurs in the ARC_EVENT_INDEX tablespace. Compare this to ARC_EVENT_DATA, where most write operations are somewhat sequential and read operations are random. Both write and read operations in ARC_EVENT_INDEX are random.

ARC_UNDO

This tablespace is used instead of Oracle's default tablespace UNDO. Because there can be only one active tablespace, once ARC_UNDO is created successfully, the ArcSight Database Configuration Wizard flags the default UNDO tablespace UNDOTBS1 as inactive. Keep UNDOTBS1 in the database in case ARC_UNDO gets corrupted.

ARC_TEMP

The ARC_TEMP tablespace stores temporary query results; for example, sorting. This tablespace is typically moderate in size and I/O load.

Volume 3: REDO Volume

The REDO volume holds Oracle redo logs. These logs are written at a high rate, and sequentially. They are read during database startup, redo log archiving, and during recovery, all of which are not relevant during everyday operation.

The ArcSight Database Installer creates three or four redo log groups (each with a single member). The number of redo log files and their default sizes depend on the template used to create the ArcSight Database. If you anticipate frequent data updates, increase the size to 3 MB each or add an additional redo log group.

You must always create a separate REDO volume to hold redo logs. Do not use the DATABASE volume for this purpose.

Given the small size but high I/O load, either high-performance direct-attached storage or NAS/SAN technology are typically used for the REDO volume.

Volume 4: ARCHIVE Volume

This volume can be split into two volumes:

- For archived Oracle redo logs
This volume is required only if Oracle is running in ARCHIVELOG mode, which is required for hot backup.
- For ArcSight partition archives

This volume is required only if Partition Archiver is enabled.



Not all ESM versions or ArcSight Express models support the Partition Archiver.

ArcSight Partition Archives

This volume holds a directory with archived partitions. Archived partitions contain event data, typically one day's worth per partition. They are compressed using zip, bzip2 or gzip. When brought back online (through the ArcSight Console), the files are decompressed in the same directory and made available to Oracle.

Typically, contents are written to the archived partitions directory once a day when the oldest online partition is archived. When a partition is reactivated, it is decompressed in this directory and queries against data in this partition are run against the ARCHIVE volume. No additional data can be inserted into this partition.

Given the large size but typically low I/O rate, inexpensive near-line storage or SATA-based SAN volumes are often used for the ARCHIVE volume.

Archived Oracle Redo Logs

This volume is required only if automatic redo log archiving is enabled, which ArcSight recommends for production instances. Installations that perform hot backups (using a tool such as Oracle's Recovery Manager, RMAN, or Veritas Net Backup for Oracle) must enable automatic redo log archiving.

Without archived redo logs, the Oracle database may not be recoverable after a disk crash.

The size of this volume depends on the number of events. If a 2 GB redo log is filled in 30 minutes on average, you will need at least 48 GB of disk space to store one day's archived redo logs. How long you need to preserve archived redo logs depends on your backup schedule.

When automatic redo log archiving is enabled, monitor the disk space usage for the redo log archive destination and purge old archived redo logs periodically. External tools can be used to compress the archived redo logs.

If there is no available space on the redo log archive destination, Oracle will hang without warning. If this happens, make more space available by either adding capacity to the volume or by deleting old archived redo logs. When space is available, Oracle will resume (a restart is not required).

Given the large size, SATA-based SAN volumes are often used for the ARCHIVE volume. However, this volume cannot be slower than the REDO volume. Otherwise, the database may hang periodically until the redo log archiver has caught up with the redo log writer.

Oracle Control Files

By default, Oracle creates the three copies of the Control File in the same location as Oracle's default tablespaces under the Oracle software installation directory, namely `$ORACLE_HOME/oradata` on Unix and Linux, and `%ORACLE_HOME%\oradata` on Windows.

It is very important to distribute three copies of the control file to three different volumes, preferably not in `$ORACLE_HOME`, and back up the control files whenever the database structure is changed. Adding a data file, for example, represents a change to the database structure.

Selecting an ArcSight Database Template

The ArcSight Database Installation Wizard presents a range of pre-defined templates that initialize ArcSight's Database. The templates include:

Size	Use
Small	For pilot installation
Medium	Small production environments
Standard	Typical production environments
Large	Large production environments
Extra Large (X-Large)	Very large production environments (See details below.)
Extra, Extra Large (XX-Large)	Very large production environments (See details below.)

The template you select for the Oracle instance creation will depend on the capacity and performance requirements of the ArcSight security management system you want to deploy.

ArcSight Database templates specify:

- Required minimum memory capacity
- Required minimum disk space
- Number of redo logs
- Redo log file size
- Minimum sizes for ArcSight tablespaces
- Required file system types

Other factors, such as other applications to be installed on the database machine, may affect your template decision. The table below lists the assumptions and configurations for the database templates provided.

ArcSight recommends dedicating a machine to the ArcSight Database. The operating system chosen often suggests a hardware platform. For Intel-based platforms (Windows or Linux), for example, two or more P4 Xeon processors is a typical configuration.

Template	CPUs	Memory	Disk
Small (Quick Demos only)	1	512 MB	16 GB
Medium (Tests/Pilots only)	1	1 GB	32 GB
Standard (Typical Production)	2	2 GB	64 GB
Large (Large Production) 64-bit machines only	4 ²	4 GB	128 GB
X-Large (Large data files) 64-bit machines only	4	8 GB	256 GB
XX-Large (Large data files) 64-bit machines only	8	16 GB	256 GB

Minimum Disk Space assumptions:

- Disk space required for Oracle software installation is not included.
- The online retention period is set to the default value of 30 days.
- The online reserve period is set to the default value of 14 days.
- Minimum sizes for ARC_UNDO and ARC_TEMP are set to the recommended values.

For the Large template on 32-bit Windows, add the /3GB option to `boot.ini` and reboot Windows before creating the ArcSight instance.

Preparing your Platform for Database Installation

UNIX Platforms

ArcSight Database can be installed on AIX, Linux, or Solaris platforms.

If the 'oracle' group and the default Oracle software owner account (that is, 'oracle') do not exist on your database host, the database installer automatically creates them. However, if you have any restrictions or password policies in place that will prevent the installer from creating the group or the owner account, you must create them manually before launching the installer.

If the installer creates the owner account automatically, you must set a password for that account after the installation is complete.

If you created the account manually, you must make sure you set a password for the account during account creation.

Preparing a Linux System



When installing SUSE Linux, please make sure that you do **not** select SUSE's in-built option that prompts you to make SUSE Oracle-ready. If you select this option, it will create an Oracle user account which conflicts with the Oracle user account created when installing ArcSight Database.

Make sure you install the required libraries for SUSE Linux that are listed in this section.

Perform the following steps to prepare Linux for the installation of ArcSight Database:

- 1 Make sure that your Linux system meets the requirements listed in [“Supported Platforms for Database Installation and Upgrade”](#) on page 24.
- 2 Verify that the following required packages (the versions stated below or newer version of the packages) are installed:

On Red Hat Enterprise Linux 4.0, 32 bit:

```
binutils-2.15.92.0.2-13.EL4
compat-db-4.1.25-9
compat-libstdc++-296-2.96-132.7.2
gcc-3.4.3-22.1.EL4
gcc-c++-3.4.3-22.1.EL44
glibc-2.3.4-2.9
glibc-common-2.3.4-2.9
libstdc++-3.4.3-22.1
libstdc++-devel-3.4.3-22.1
make-3.80-5
sysstat-5.0.5-1
setarch-1.6-1
```

On Red Hat Enterprise Linux 4.0, 64 bit:



On 64-bit machines, you will need both the 32-bit and 64-bit versions of the libraries.

```
binutils-2.15.92.0.2-10.EL4
compat-db-4.1.25-9
compat-libstdc++-33-3.2.3-47.3
compat-libstdc++-33-3.2.3-47.3(i386)
compat-libstdc++-296.i386
gcc-3.4.3-22.1
```

```
gcc-c++-3.4.3-22.1
glibc-2.3.4-2
glibc-2.3.4-2(i386)
glibc-common-2.3.4-2
glibc-devel-2.3.4-2
glibc-devel-2.3.4-2(i386)
libaio-0.3.96-3
libgcc-3.4.3-9.EL4
libstdc++-3.4.3-9.EL4
libstdc++-devel-3.4.3-9.EL4
make-3.80-5
sysstat-5.0.5-1
```

On Red Hat Enterprise Linux 5, 32-bit

```
binutils-2.17.50.0.6-2.el5
compat-libstdc++-33-3.2.3-61
elfutils-libelf-0.125-3.el5
elfutils-libelf-devel-0.125
gcc-4.1.1-52
gcc-c++-4.1.1-52
glibc-2.5-12
glibc-common-2.5-12
glibc-devel-2.5-12
glibc-headers-2.5-12
libaio-0.3.106
libaio-devel-0.3.106
libgcc-4.1.1-52
libstdc++-4.1.1
libstdc++-devel-4.1.1-52.el5
make-3.81-1.1
sysstat-7.0.0
```

On Red Hat Enterprise Linux 5, 64-bit



On 64-bit machines, you will need both the 32-bit and 64-bit versions of the libraries.

```
binutils-2.17.50.0.6-2.el5
compat-db-4.1.25-9
compat-libstdc++-33-3.2.3-61
compat-libstdc++-33-3.2.3-61(i386)
compat-libstdc++-296(i386)
gcc-4.1.1-52.el5
gcc-c++-4.1.1-52.el5
glibc-2.5-12
glibc-2.3.4-2(i386)
glibc-common-2.5-12
glibc-devel-2.5-12
glibc-devel-2.5-12(i386)
glibc-headers-2.5-12
libgcc-4.1.1-52.el5(i386)
libaio-0.3.96-3
libgcc-4.1.1-52.el5(x86_64)
libstdc++-3.4.3-9.EL4
libstdc++-devel-3.4.3-22.1
libgomp-4.1.1-52.EL5
make-3.81-1.1
sysstat-7.0.0-3.el5.x86_64.rpm
```

On SUSE Linux Enterprise Server 10, 64 bit:

```
binutils-2.16.91.0.5-23.31
compat-libstdc++-5.0.7-22.2
gcc-4.1.2_20070115-0.21
gcc-c++-4.1.2_20070115-0.21
glibc-2.4-31.54
glibc-devel-2.4-31.54
glibc-devel-32bit-2.4-31.54
```

```
glibc-32bit-2.4-31.54
libaio-32bit-0.3.104-14.2
libaio-0.3.104-14.2
libaio-devel-0.3.104-14.2
libelf-32bit-0.8.5-47.2
libgcc-4.1.2_20070115-0.21
libstdc++-4.1.2_20070115-0.21
make-3.80-202.2
```



If any of these packages are not installed, you may want to reinstall Linux.

On SUSE Linux Enterprise Server 11:

```
make-3.81-128.20
binutils-2.19-11.28
gcc-32bit-4.3-62.198 (i386)
gcc-4.3-62.198
gcc-c++-4.3-62.198
libaio-0.3.104-140.22
libaio-devel-0.3.104-140.22
libaio-32bit-0.3.104-140.22 (i386)
libaio-devel-32bit-0.3.104-140.22 (i386)
glibc-32bit-2.9-13.2
glibc-2.9-13.2
glibc-devel-2.9-13.2
glibc-devel-32bit-2.9-13.2 (i386)
glibc-devel-2.9-13.2
glibc-devel-32bit-2.9-13.2 (i386)
libstdc++-devel-4.3-62.198
```

- 3 Remember to run the ArcSight Database Installer as root for the installation to be successful.

- 4 Make sure that the ports listed in the [“Protecting ArcSight Manager” on page 12](#) are open in order to facilitate a smooth communication between the ArcSight Manager and the database.



Red Hat Linux 4 has firewall enabled by default, which will cause the ArcSight setup and configuration programs to fail. Since ArcSight Manager needs to communicate with the database machine, you must open the ports listed in the [“Protecting ArcSight Manager” on page 12](#) on the Manager and database machines before proceeding with the ArcSight Manager setup.

- 5 Run the `hostname` command and check that it returns the fully-qualified host name in the form “hostname.domainname.”

If not, do the following:

- a Set the host name to a fully-qualified name with the following command:

```
hostname hostname.domainname
```

- b Edit the file `/etc/sysconfig/network` to set the host name to the same fully-qualified name permanently.

- 6 Check `/etc/hosts` and make sure the entry for localhost is “127.0.0.1 localhost.localdomain localhost”.
- 7 Run the `ping` command to verify the host names for both the Manager machine and the database machine are resolvable from both sides.
- 8 Make sure that you have selected at least the “minimal” package group option while configuring your RHEL4u6 AS 32bit system.
- 9 Make sure that you have selected at least the “default” package group option while configuring your RHEL4.0 AS 64-bit system.

Preparing a Solaris System

Perform the following steps to prepare Solaris for the installation of ArcSight Database:

- 1 Make sure that your Solaris system meets the requirements listed in [“Supported Platforms for Database Installation and Upgrade” on page 24](#).
- 2 Log in as root and run the `ulimit -a` command to view the currently defined system limits. Make sure that the limits below are set to the following:
 - ◆ Set the “cpu time” to “unlimited”
 - ◆ Set the “file size” to “unlimited”
 - ◆ Set the “data seg size” to “unlimited” or to at least “1048576”
 - ◆ Set the “stack size” to at least “32768”
 - ◆ Set the “open files” to at least “4096”
 - ◆ Set the “virtual memory” to “unlimited” or to at least “4194304”
- 3 Remember to run the ArcSight Database Installer as root in order for the installation to be successful.
- 4 Make sure that you choose the Developer package when installing Solaris so that Oracle will be able to link its executables during the installation process. Make sure the

command `/usr/sbin/prtconf` is available and that `/usr/sbin` is included in root's shell environment variable `PATH`.



Instead of installing the Developer package, you can install the following packages in your environment: `SUNWlibm`, `SUNWlibms`, `SUNWsprot`, `SUNWtoo`, `SUNWi10f`, and `SUNWXwfnt`.

5 Verify that the following required packages are installed:

On Solaris 10 64 bit:

`SUNWarc`
`SUNWbtool`
`SUNWhea`
`SUNWlibm`
`SUNWlibms`
`SUNWsprot`
`SUNWtoo`
`SUNWilof`
`SUNWilcs`
`SUNWi15cs`
`SUNWxfnt`
`SUNWsprox`

You can run the following Solaris command to check whether these packages are installed or not:

```
# pkginfo -i SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms
SUNWsprot SUNWsprox SUNWtoo SUNWilof SUNWilcs SUNWi15cs
SUNWxfnt
```

You should also apply the latest Solaris Operating System patches. Check <http://sunsolve.sun.com> for Solaris patches.

6 If Perl is not installed, download the binary distribution from <ftp://ftp.sunfreeware.com/pub/freeware/sparc> and install it.



The Oracle patchset installer also requires the `SUNWuiu8 Iconv` modules for UTF-8 locale, and the `SUNWuiu8x Iconv` modules for UTF-8 locale (64-bit).

7 The installer edits `/etc/system` to specify kernel parameters for shared memory segments and semaphores which Oracle uses at startup. Lines that start with "set shmsys:" or "set semsys:" are deleted and the following lines are added, replacing `SHMMAX` with the total memory required by the ArcSight Database Template you selected, in bytes. (Multiplied by 1,048,576 to convert megabytes to bytes.)

```
set shmsys:shminfo_shmmax=SHMMAX
set shmsys:shminfo_shmmin=1
```

```
set shmsys:shminfo_shmmni=512

set shmsys:shminfo_shmseg=64

set semsys:seminfo_semmns=512

set semsys:seminfo_semmni=512

set semsys:seminfo_semopm=64

set semsys:seminfo_semmsl=1024

set semsys:seminfo_semvmx=32767
```

The installer will prompt you to reboot for changes to `/etc/system` to take effect.

Preparing a Windows System

Perform the following steps to prepare Windows for the installation of ArcSight Database:

- 1 Make sure that your Windows system meets the requirements listed in “[Supported Platforms for Database Installation and Upgrade](#)” on page 24.
- 2 ArcSight requires a clean database machine. If Oracle was previously installed on the database machine, reinstall the operating system before proceeding further.
- 3 Remember to run the ArcSight Database Installer as the local ‘Administrator’ user for the installation to be successful.

Installing or Upgrading ArcSight Database and Oracle



Tools that require a remote login to a Manager running in FIPS mode will need to be run from the Manager's `<ARCSIGHT_HOME>` as opposed to the database's `<ARCSIGHT_HOME>`. However, running these tools in a standalone mode by stopping the Manager and running the tools directly on the database is supported.



ESM v4.5 does not support Oracle 9x. If your current ESM installation uses Oracle 9x, you are required to upgrade it to Oracle 10g. If you would like to upgrade to Oracle 10.2.0.4, you will be required to first upgrade your Oracle software to a minimum of Oracle 10.2.0.2 **before** you upgrade to Oracle 10.2.0.4.

To upgrade to Oracle 10.2.0.2, run the following command from the ESM v4.0 SP1 ArcSight Database `bin` directory:

```
arcsight databasesetup
```

and follow the wizard screens. Select **Upgrade Oracle 9i instance to 10gR2** when prompted. See the *ArcSight Installation and Configuration Guide, v4.0 SP1* for details.

Once you have upgraded to Oracle 10.2.0.2, you can use the ESM v4.5 ArcSight Database software to upgrade to Oracle 10.2.0.4



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.

The installation or upgrade process involves these steps:

- 1 Install the ArcSight Database software.

2 Depending on your current setup, select from one of these actions:

- ◆ A brand new install
- ◆ A new ArcSight install that will use pre-existing Oracle 10g software
- ◆ A new ArcSight installation that will use pre-existing Oracle 10g software and a 10g instance
- ◆ An existing ArcSight installation with Oracle 10g software and a 10g instance (that is, an upgrade candidate)



If you choose to upgrade from Oracle 10.2.0.2 to 10.2.0.4, make sure that you have Oracle 10gR2 installed on your system. Otherwise you will encounter an error message.

The wizards for each of these actions are described in detail next.



If the database installation or upgrade process exits at any step in the following procedure, you can restart it with this command:

`arcsight database install`

Installing the ArcSight Database Software

Once you have prepared your system as described earlier in this chapter and read the prerequisites, you are ready to install or upgrade the ArcSight Database component and, if needed, the Oracle 10g database software.

Follow these steps to install the ArcSight Database software:

- 1 Download the ArcSight Database installation file, and if needed, the Oracle 10g database files appropriate for your platform from <https://software.arcsight.com>. Copy all the files (without extracting their contents) to a temporary directory.

The following files are available.

Platform	Oracle 10g Database Files	
	64-bit	32-bit
Windows	AMD64: 102010_win64_x64_database.zip p6810189_10204_MSWIN-x86-64.zip	IA32: 10201_database_win32.zip p6810189_10204_win32.zip
Linux	AMD64: 10201_database_linux_x86_64.cpio.gz p6810189_10204_Linux-x86-64.zip	IA32: 10201_database_linux32.zip p6810189_10204_Linux-x86.zip
Solaris	10gr2_db_sol.cpio.gz p6810189_10204_SOLARIS64.zip	

Platform	Oracle 10g Database Files
AIX	10gr2_aix5l64_database.cp io.gz p6810189_10204_AIX5L

Platform	ArcSight Installation file
Windows	ArcSight-4.5.x.nnnn.y-DB-Win.exe
Linux	ArcSight-4.5.x.nnnn.y-DB-Linux.bin
Solaris	ArcSight-4.5.x.nnnn.y-DB-Solaris.bin
AIX	ArcSight-4.5.x.nnnn.y-DB-AIX.bin

- 2 Run the appropriate self-extracting ArcSight installation file for your platform.



Note

A Windows system was used for the sample installation. If you are installing your database on a Unix based system, you will notice a few Unix-specific screens.

Screens that summarize your selections or the ones that report progress on the installation are not shown in this sample installation.

- 3 Read the introduction and click **Next**.
- 4 Read the notice and click **Next**.
- 5 Choose a directory in which to install ArcSight Database and click **Next**.



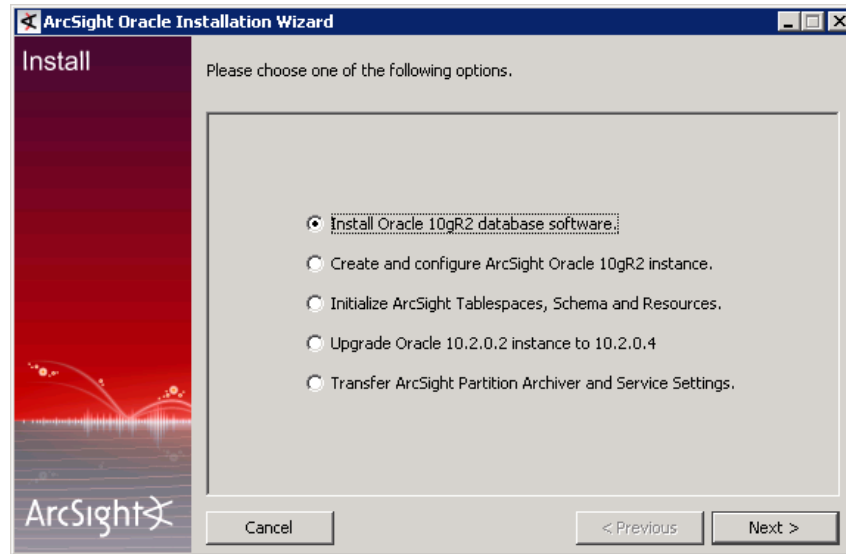
Caution

If the directory you choose already exists, the installer will clear any contents that exist in the directory. If you do not want to delete the existing contents of the directory, you may want to specify a new location for the current installation.

- 6 Choose a location where you would like to create a shortcut for ArcSight Database and click **Next**.
- 7 Check to make sure that the folder locations in the Pre-installation Summary are correct and click **Install**.

You will see a screen in which shows you the progress of the installation. The Oracle configuration wizard opens after the installation is complete.

- 8 In the following screen, select from one of the following options. The following table will help you select the option appropriate for you.



Current Setup	Use This Option
A new install	#1—Install Oracle 10gR2 database software. Refer to “Installing Oracle 10g Database Software” on page 42.
A new ArcSight installation that will use a pre-existing Oracle 10g software	#2—Create and configure ArcSight Oracle 10gR2 instance. Refer to “Creating a New Oracle 10g Instance” on page 45.
A new ArcSight installation that will use a pre-existing Oracle 10g software and a 10g instance	#3—Initialize ArcSight Tablespaces, Schema, and Resources. Refer to “Initializing ArcSight Tablespaces, Schema, and Resources” on page 50.
An existing ArcSight installation with Oracle 10.2.0.2 software and a 10.2.0.2 instance	#4—Upgrade Oracle 10.2.0.2 Instance to 10.2.0.4. Refer to the ESM Upgrade Guide for instructions on upgrading your Oracle software.
An existing ArcSight installation with Oracle 10.2.0.2 instance and an Oracle 10.2.0.2 software	#5—Transfer ArcSight Partition Archiver and Service Settings

If you chose option #1, go to [“Installing Oracle 10g Database Software”](#) on page 42.

If you chose option #2, go to [“Creating a New Oracle 10g Instance”](#) on page 45.

If you chose option #3, go to [“Initializing ArcSight Tablespaces, Schema, and Resources”](#) on page 50.



Note

If you do not have root access to your database machine, you will not be able to initialize tablespaces, schema, and resources using this interface. To initialize tablespaces, schema, and resources in that case, run this command in `<ARCSIGHT_HOME>\bin`:

```
arcsight database init
```

If you chose option #4, follow the instructions in the ESM Upgrade Guide to upgrade your Oracle software.



If you choose to upgrade from Oracle 10.2.0.2 to 10.2.0.4, make sure that you have Oracle 10gR2 installed on your system. Otherwise, you will encounter an error message.

You can ignore option #5. This option is used to transfer Partition Archiver settings from an existing installation and is only applicable if you are upgrading ArcSight Database.



Not all ESM versions or ArcSight Express models support the Partition Archiver.

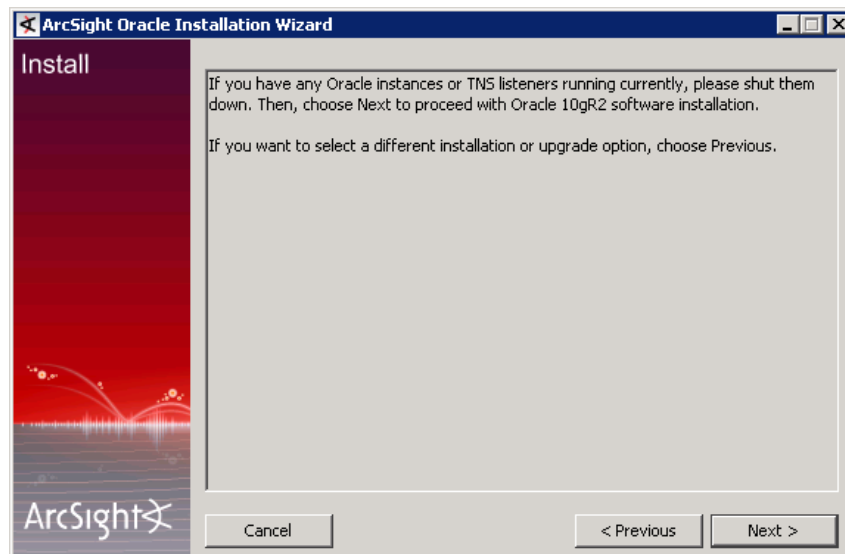
Installing Oracle 10g Database Software



If you are upgrading from Oracle 10.2.0.2 to Oracle 10.2.0.4 and you want to keep the Oracle 10.2.0.2 installation, you need to specify a new path for the "Oracle Installation Directory" in the ArcSight Oracle Installation Wizard at the appropriate screen.

If the directory you choose already exists, the installer will clear any contents that exist in the directory. If you do not want to delete the existing contents of the directory, you may want to specify a new location for the current installation.

- 1 The following screen prompts you to shut down currently running Oracle instances or TNS listeners.



To shut down TNS listeners, run this command on the database machine:



Make sure you have set the environment variables `ORACLE_HOME` and `ORACLE_SID` to appropriate values before running the commands below.

```
% arcdbutil lsnrctl stop
```

To shut down an Oracle instance, run this command on the database machine:

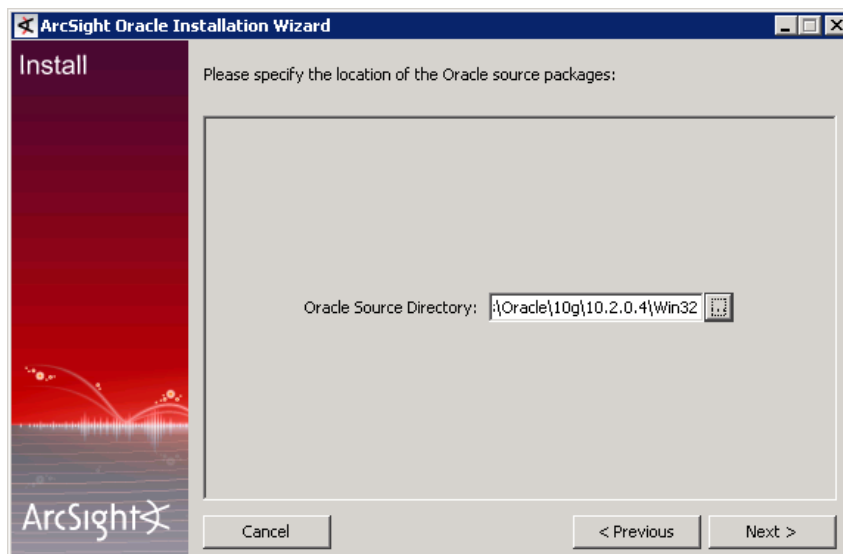
```
% arcdbutil sql
```

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

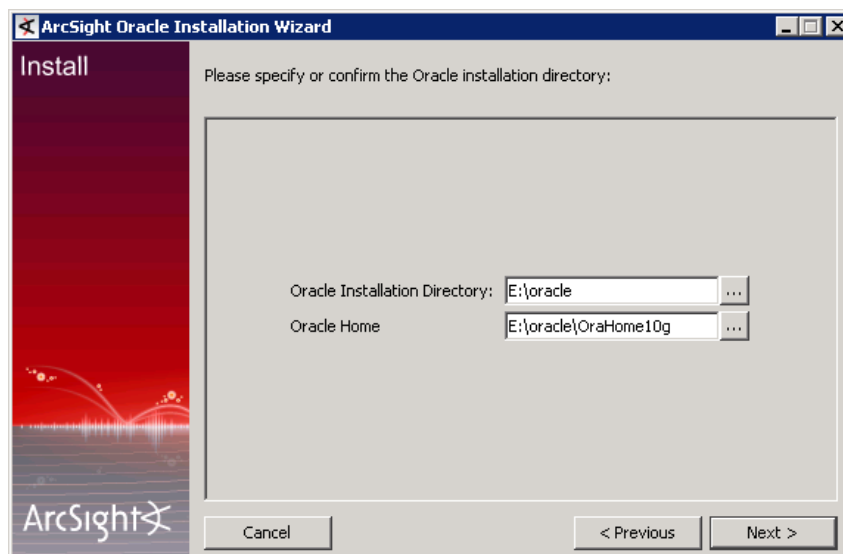
```
SQL> shutdown immediate
```

```
SQL> exit
```

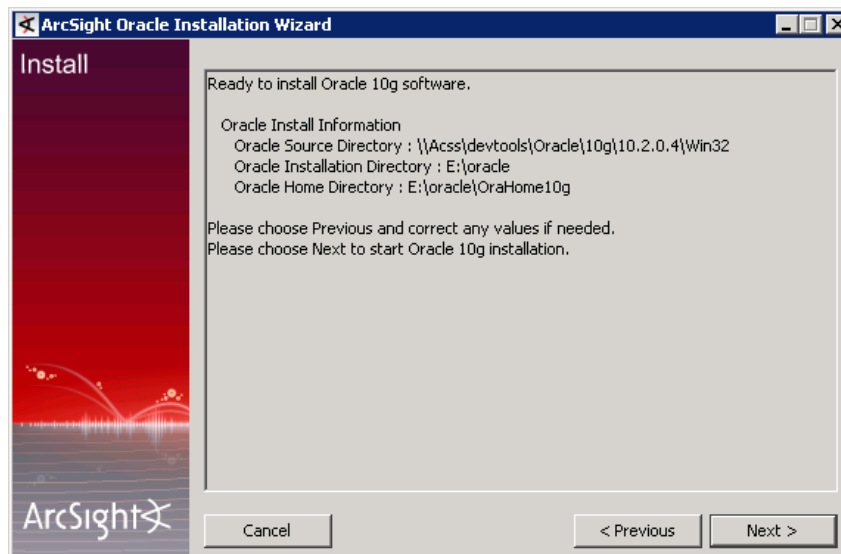
- 2 Enter the location where you copied the Oracle 10.2.0.4 database software files in Step 1 of ["Installing the ArcSight Database Software" on page 39](#) and click **Next**:



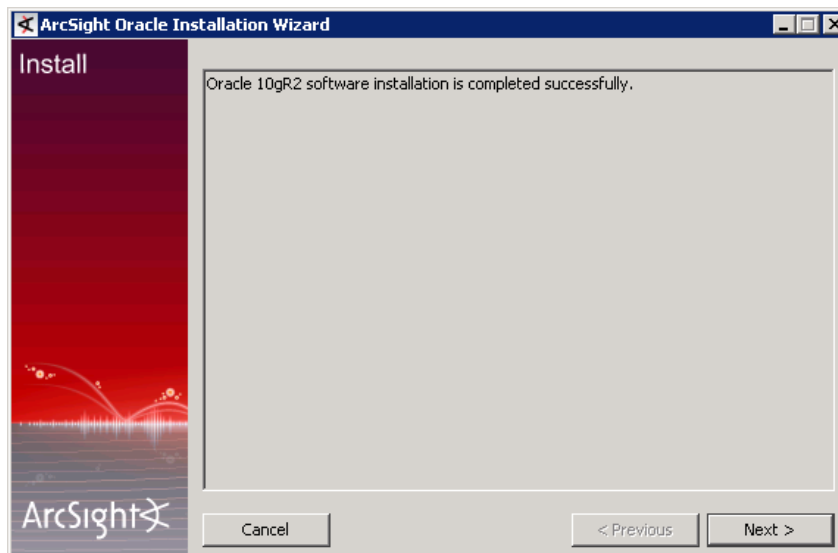
- 3 Specify or confirm Oracle installation directory and click **Next**:



- 4 Make sure that all the locations you specified are correct and click **Next**.



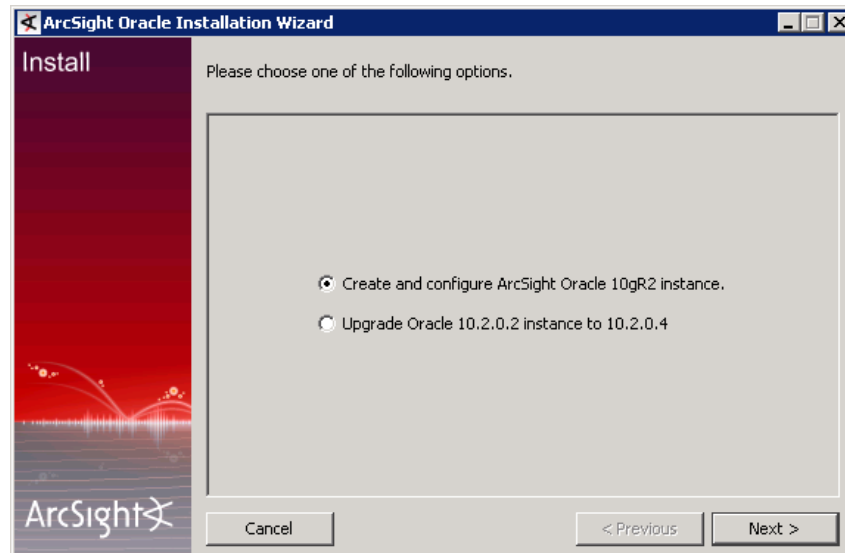
You will see the following screen when the Oracle installation completes. Click **Next** to configure an ArcSight Oracle instance.



- 5 Select whether you want to create and configure the ArcSight Oracle instance or you want to upgrade an existing Oracle 10.2.0.2 instance. In the following screen, select from one of the following options. The following table will help you decide the option to select.

Current Setup	Use This Option
A new install	<p>#1—Create and configure ArcSight Oracle 10gR2 instance</p> <p>If you choose this option, follow the procedure described in “Creating a New Oracle 10g Instance” on page 45.</p>

Current Setup	Use This Option
An existing ArcSight installation with Oracle 10.2.0.2 database and a 10.2.0.2 instance	<p>#2—Upgrade Oracle 10.2.0.2 instance to 10.2.0.4</p> <p>If you choose this option, go to the ESM Upgrade Guide and follow the instructions to upgrade your Oracle instance.</p>



Creating a New Oracle 10g Instance



Note

Setting the Database Block Size: ArcSight embedded Oracle installer will create the instance with a default block size of 16K. Note that the database block size is a parameter that can only be configured BEFORE the instance has been created. If you determine that your Operating System and hardware would function more optimally with a different block size, you will have to edit the ArcSight template to change the block size. Before you choose to create the ArcSight Oracle instance, edit the file in `<ARCSIGHT_HOME>\installer\Oracle10g\<platform>\dbca\ArcSight_<size>.dbt` in a text editor. Search for "db_block_size" and replace its default value "16384" with, for example, "32768" for a 32K block size.

- 1 If you are creating a new instance, you will need to enter the following parameters in the next screen.

ORACLE_SID—System ID (SID) for the ArcSight Database. By default, arcsight. The global database name and the TNS service name will be set to the value you specify for this parameter. The Oracle SID cannot exceed 8 characters.

ArcSight Database Template—The template that determines the configuration (for example, memory allocation) of the ArcSight Database you want to create. By default, `ArcSight_Standard.dbt` (Standard).

Depending on the platform, you can choose from XX-Large, X-Large, Large, Standard, Medium, and Small. For more information about ArcSight Database templates, see [“Selecting an ArcSight Database Template” on page 30](#).

Database Character Set—The language that Oracle should use to operate; for example, English. By default, your operating system setting.

Allowed TNS Clients—A comma-separated list of host names or IP addresses that are allowed to connect to this database.



Note

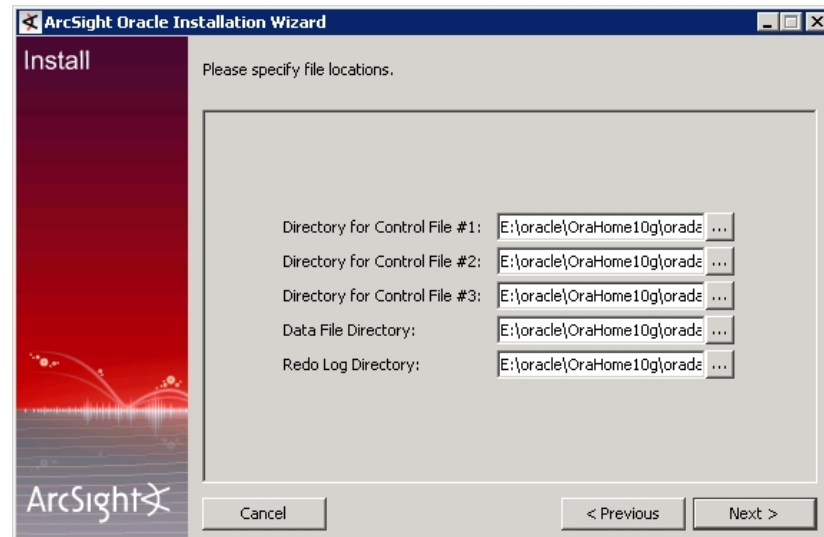
The database machine will only accept connection requests from the specified client list. If the ArcSight Manager is running on another host (as recommended), you must include both the 'localhost' and the ArcSight Manager host in the list. The installer automatically replaces 'localhost' with the actual IP address of the local host. By default, localhost.

- 2 Enter the following parameters in the next screen. Although default directory locations are filled for you, ArcSight recommends that you specify directory locations on separate disks for each of these files to prevent loss from hard disk failures.

Directory for Control File #1, #2, and #3-- The directories where the copies of Oracle's control files are stored. By default, `<ORACLE_HOME>\oradata\ORACLE_SID`.

Data File Directory-- The directory where default data files for Oracle's Data Dictionary will be stored. You need at least 400 MB available disk space for this directory. By default, `<ORACLE_HOME>\oradata\ORACLE_SID`.

Redo Log Directory-- The directory where Oracle's redo logs will be stored. By default, <ORACLE_HOME>\oradata\ORACLE_SID.



- 3 Specify the following redo archive options in the next screen:

Auto Archive Redo Log-- Specify whether to enable automatic log archiving. Note that Redo log archiving requires a large amount of additional disk space and will impact database performance. Therefore, you should only enable log archiving in situations where you cannot tolerate any loss of data from disk crashes. By default, no.

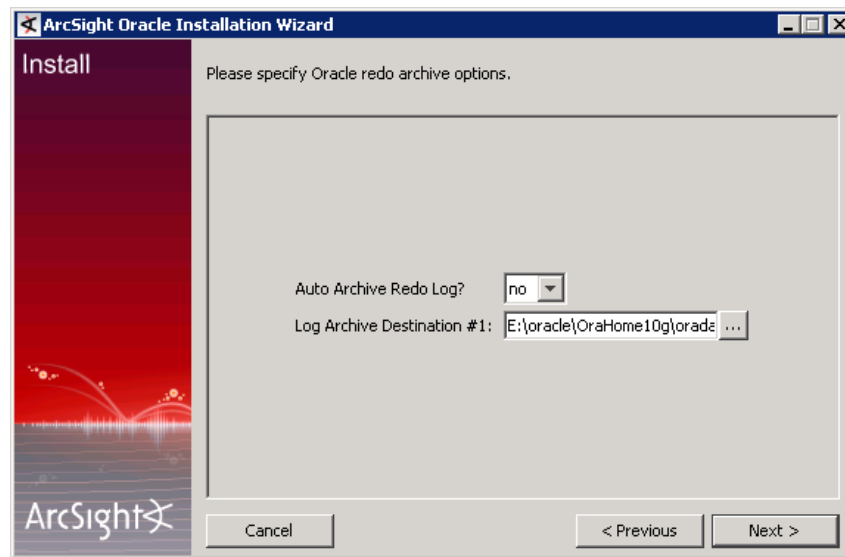
Log Archive Destination #1-- The directory to store archived redo log files if you enabled automatic redo log archiving.

Oracle can store archive redo logs in multiple log archive destinations (directories or services) simultaneously for redundancy or other purposes. You can add up to 9 more different log archive destinations later, manually.



Caution

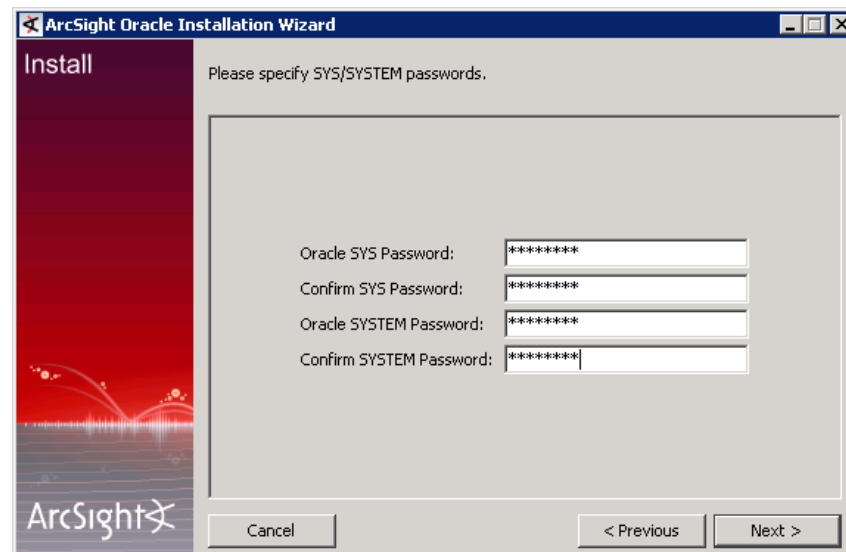
The log archive destination cannot be on a raw disk partition.



- 4 Enter the following information for the next screen:

Oracle SYS Password—Password for the Oracle superuser, SYS. By default, none.

Oracle SYSTEM Password—Password for the Oracle admin account. By default, none.



- 5 Enter the following information for the next screen which collects the passwords for the system user accounts:



Note

If you select **no** as your answer to the question “Install Enterprise Manager?”, you do not need to enter the Oracle DBSNMP and Oracle SYSMAN passwords.

Oracle DBSNMP Password— Password for the Management Agent component of Oracle Enterprise Manager used to monitor and manage the database.

Oracle SYSMAN Password— Password for the default super user account used to set up and administer Enterprise Manager.



Although you can install the Oracle Enterprise Manager client using ArcSight's Oracle 10g Installer, you must acquire licensing and support from Oracle directly.

ArcSight Oracle Installation Wizard

Install

Please specify Enterprise Manager options.

Install Enterprise Manager ? no

Oracle DBSNMP Password:

Confirm DBSNMP Password:

Oracle SYSMAN Password:

Confirm SYSMAN Password:

Cancel < Previous Next >

Click **Next** to continue.

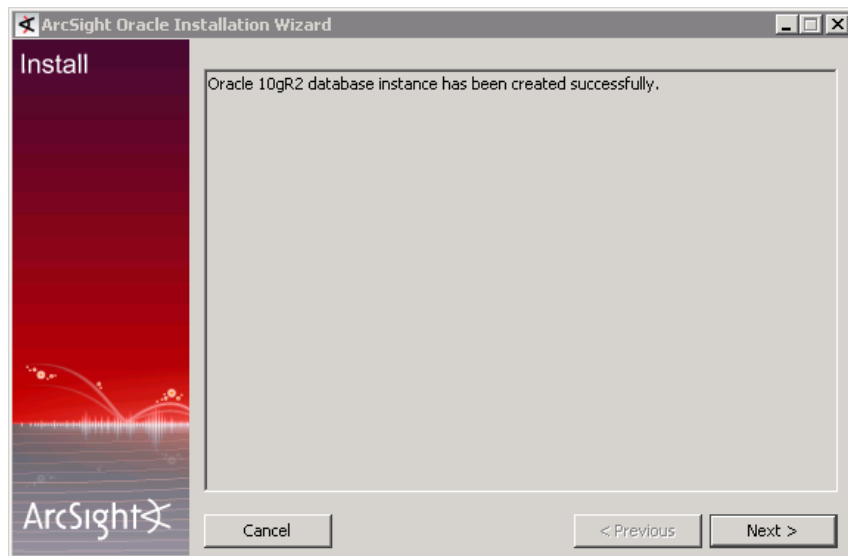
ArcSight Oracle Installation Wizard

Install

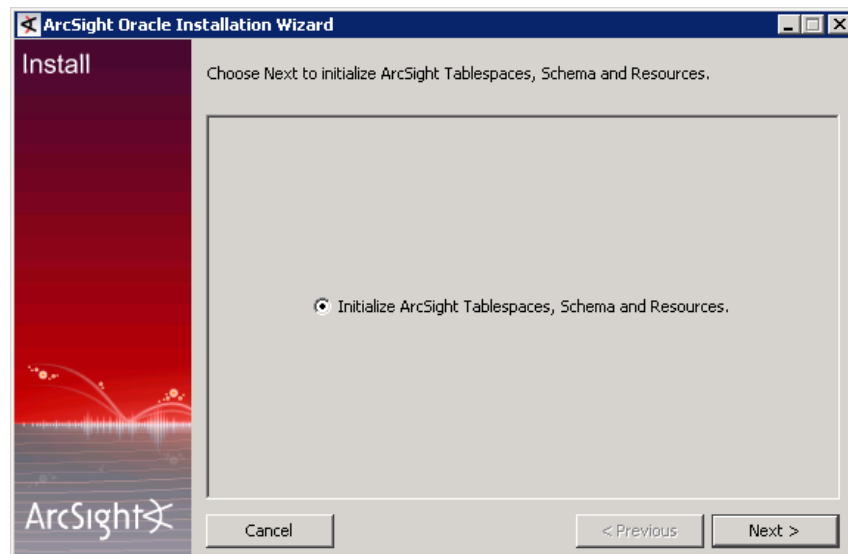
Ready to create Oracle instance.

Choose Next to start the Oracle instance creation or Previous to go back and make changes.

Cancel < Previous Next >



- 6 Click **Next** to start initializing ArcSight tablespaces, schema, and resources. Follow the procedure described in [“Initializing ArcSight Tablespaces, Schema, and Resources”](#) on page 50.



Initializing ArcSight Tablespaces, Schema, and Resources

- 1 You must check the status of the TNS listener and Oracle 10g instance to make sure they are up and running. The following screen prompts you to do so.

To check the TNS listener, run this command on the database machine:

```
% arcdbutil lsnrctl status
```

If the TNS listener is not up, run this command to start it:

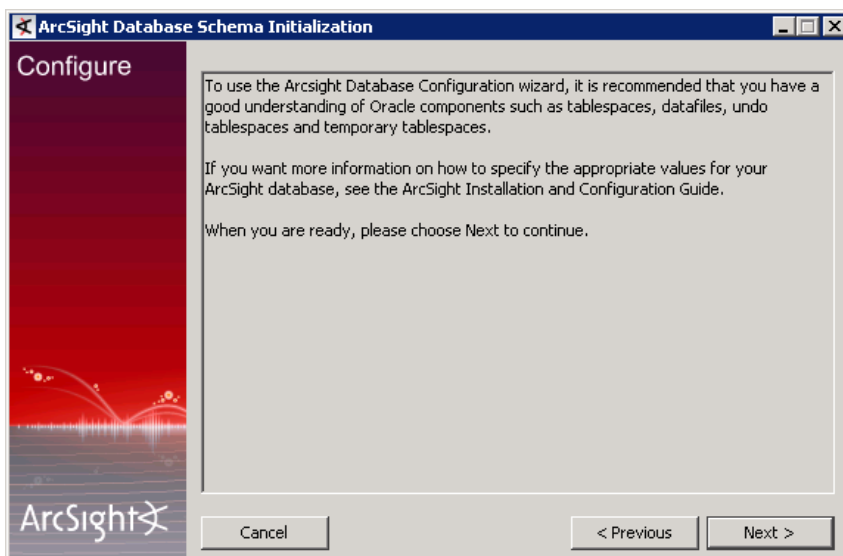
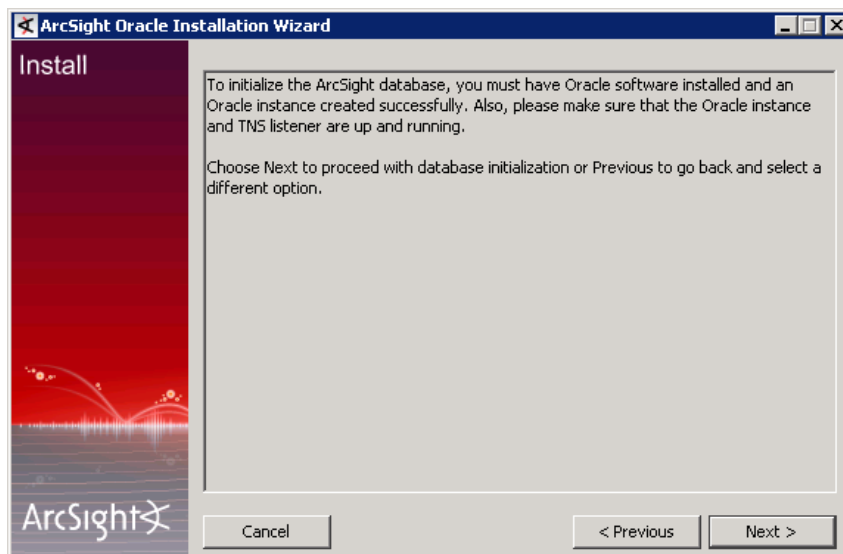
```
% arcdbutil lsnrctl start
```

To check the status of the Oracle instance, run this command on the database machine:

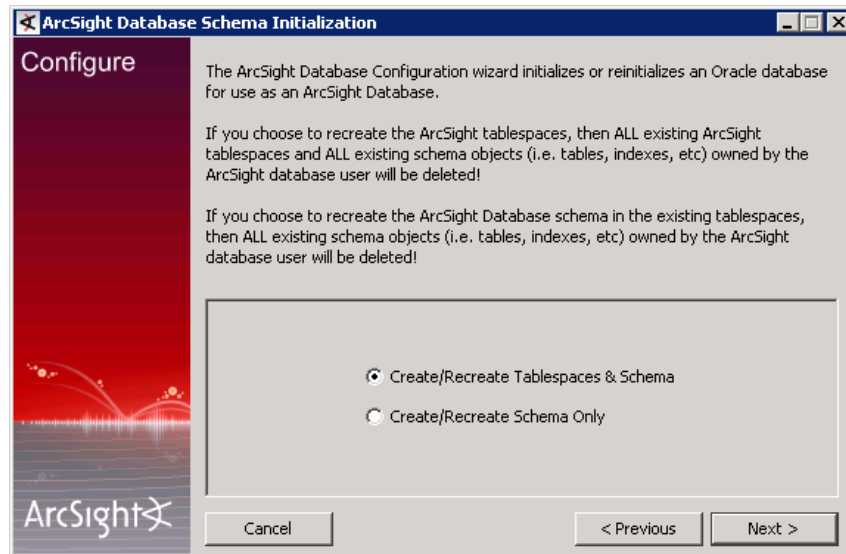
```
% arcdbutil sql  
Enter user-name: / as sysdba  
SQL> select * from dual;  
SQL> exit
```

To start the Oracle instance, run this command on the database machine:

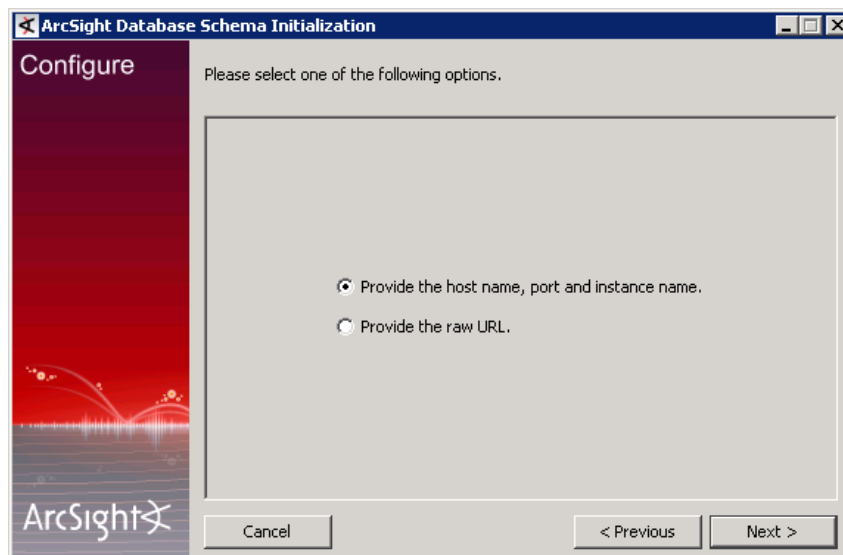
```
% arcdbutil sql  
Enter user-name: / as sysdba  
SQL> startup immediate  
SQL> exit
```



- 2 Select the first option, **Create/Recreate Tablespaces and Schema**, to create table spaces for your Oracle instance and the ArcSight Schema.



- 3 Select the first option to provide the host name, port and instance name.



- 4 Enter the following information in the next screen:



Caution

Please keep in mind that Oracle supports only alphanumeric characters for database user names, and will not accept a dash (-) or underscore (_) in these names.

Database Host Name—The IP address of the machine on which you are installing the database.

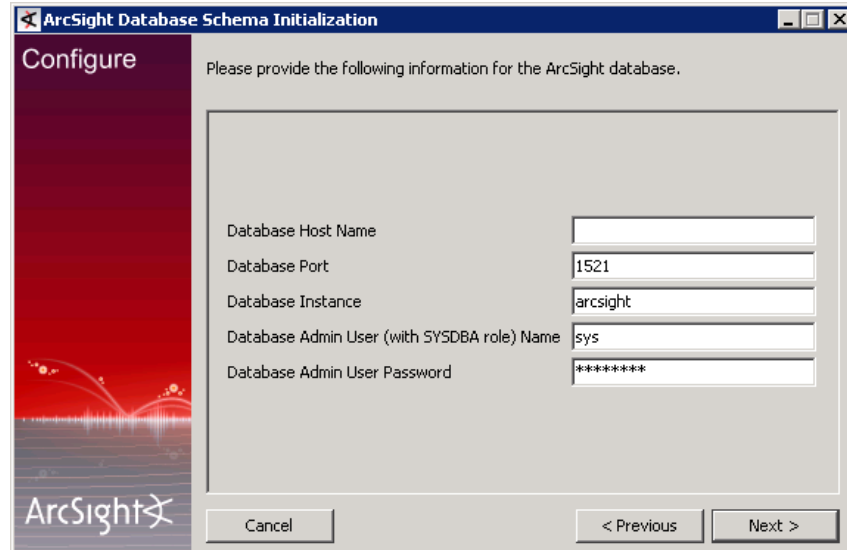
Database Port—The TCP port number on which the Oracle listener listens for connections. By default, 1521.

Database Instance—The Oracle database instance System ID (SID) that you specified when you created the Oracle instance earlier.

Database Admin User Name—The Oracle super user name. By default, SYS.

Database Admin User Password—The password for the Oracle super user account.

Database OS user name—The Oracle user name you specified when installing the database. By default, oracle.

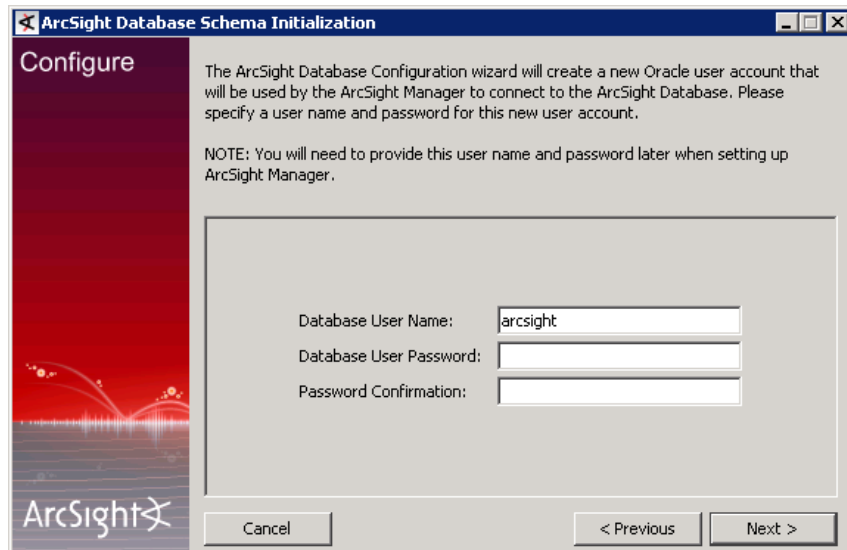


The screenshot shows the 'ArcSight Database Schema Initialization' window with the 'Configure' tab selected. The window title is 'ArcSight Database Schema Initialization'. The left sidebar has a red background with the ArcSight logo. The main area contains the text: 'Please provide the following information for the ArcSight database.' Below this is a form with the following fields:

Database Host Name	<input type="text"/>
Database Port	<input type="text" value="1521"/>
Database Instance	<input type="text" value="arcsight"/>
Database Admin User (with SYSDBA role) Name	<input type="text" value="sys"/>
Database Admin User Password	<input type="password" value="*****"/>

At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

5 Enter a Database User Name and User Password.



The screenshot shows the 'ArcSight Database Schema Initialization' window with the 'Configure' tab selected. The window title is 'ArcSight Database Schema Initialization'. The left sidebar has a red background with the ArcSight logo. The main area contains the text: 'The ArcSight Database Configuration wizard will create a new Oracle user account that will be used by the ArcSight Manager to connect to the ArcSight Database. Please specify a user name and password for this new user account.' Below this is a note: 'NOTE: You will need to provide this user name and password later when setting up ArcSight Manager.' Below the note is a form with the following fields:

Database User Name:	<input type="text" value="arcsight"/>
Database User Password:	<input type="password"/>
Password Confirmation:	<input type="password"/>

At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

6 Enter the name for System User

During the installation process, a set of predefined content called the System Core content is installed by default. This content provides the foundation building blocks for the ArcSight ESM system to work.

System Core content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in [/All Filters/ArcSight System/Core](#).

The modification of System Core content can adversely impact the operation of ArcSight ESM, therefore, it is locked by default. ArcSight strongly recommends against

unlocking or modifying this content. However, a special user called the system user is created automatically during the installation. This user can lock and unlock ArcSight Core Content if there is a need.

The system user is configured as 'systemuser' by default. ArcSight recommends that you change this name to a non-standard name. This name can be changed only once. For example, once you change the name to 'coreuser', you cannot change this name again.

If you want to change the name of system user, enter a new name in the following screen and click **Next**.

7 Enter information for these tablespaces in the next few screens:

- ◆ ARC_SYSTEM_DATA
- ◆ ARC_SYSTEM_INDEX
- ◆ ARC_EVENT_DATA
- ◆ ARC_EVENT_INDEX
- ◆ ARC_UNDO
- ◆ ARC_TEMP

For information about these table spaces, see ["Volume 2: DATABASE Volume" on page 26](#).

Enter the following information for each tablespace:

Data File Path—The directory where the data files for this tablespace will be created. The user that runs Oracle (typically, oracle) needs to have write privileges on this directory.

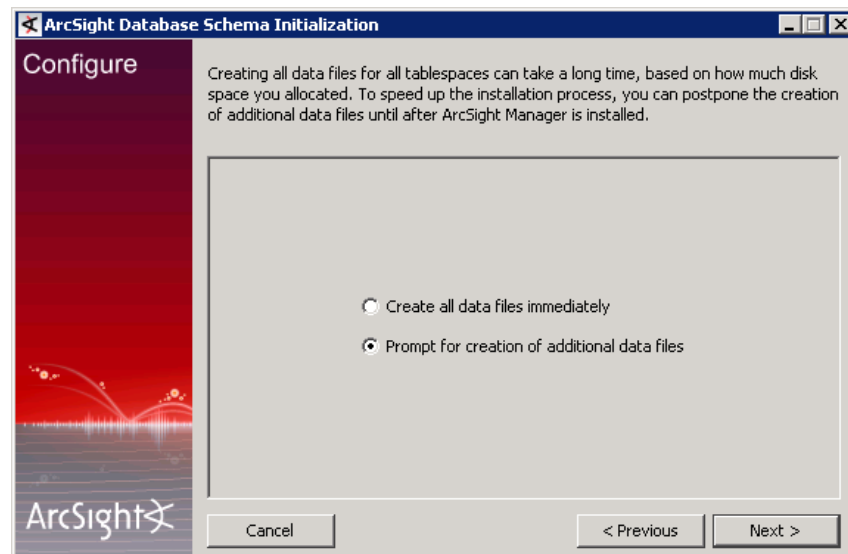
Data File Size—The size of each individual data file.

Number of Data Files—The number of data files that will be created for the tablespace.

8 Because the creation of all data files for all tablespaces can be time consuming, the following screen gives you an option to create the minimum number of files per tablespace—that is, one file per tablespace—and delay the creation of additional files until after you have completed the database configuration process. ArcSight recommends selecting the option to delay the creation of additional files.

Create all data files immediately—Create all files before proceeding further.

Prompt for creation of additional data files—Delay the creation of additional data files.

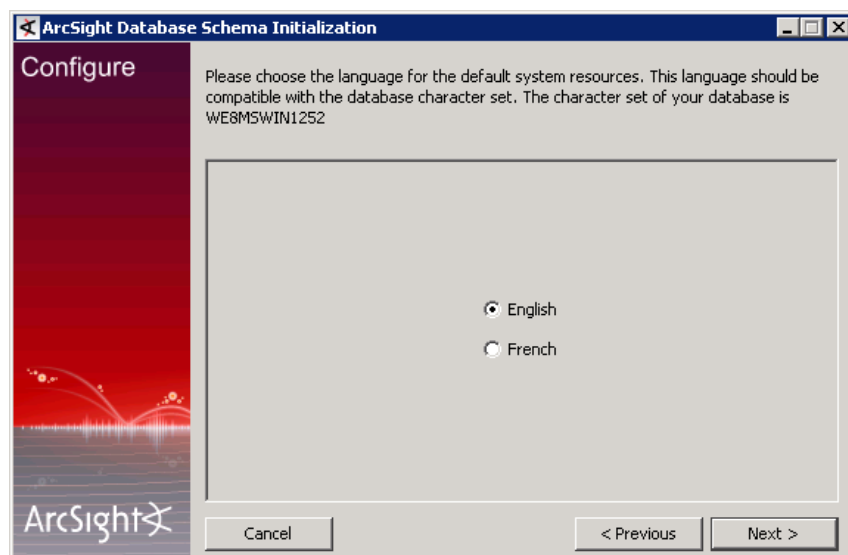


- 9 In [Step 1 on page 45](#) if you had chosen a database character set that supports more than one language supported by ESM, you will see the following screen requesting you to select a language for installing your system resources in:

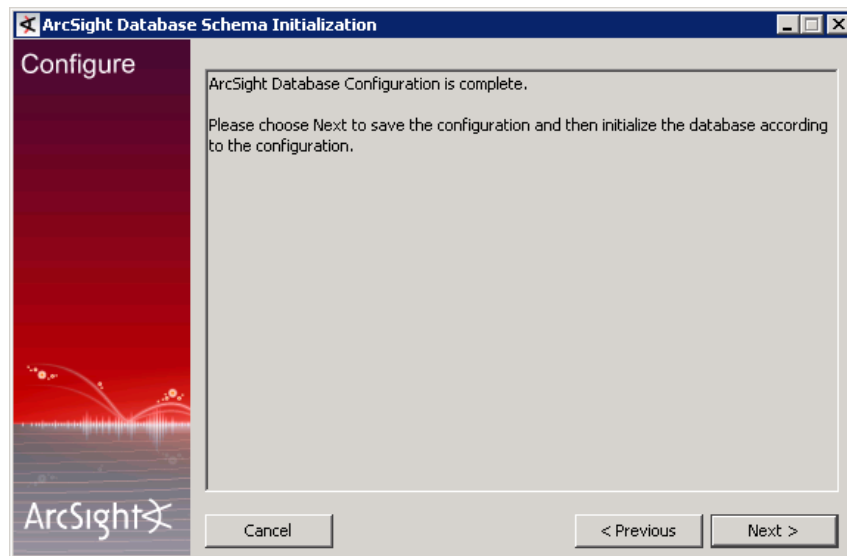


Note

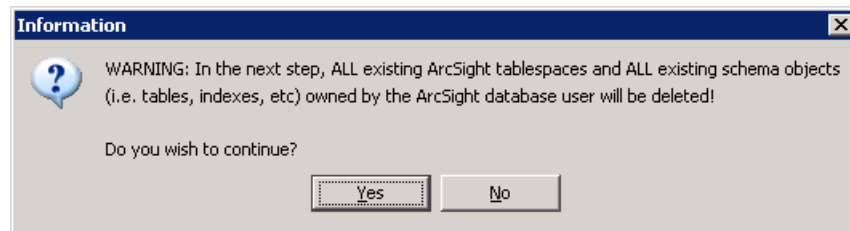
The choices for language selection in the screen below will vary depending upon the character set you selected. The choices shown in the screenshot below appear if you selected UTF8 character set.



- 10 Click **Next** to save the configuration.

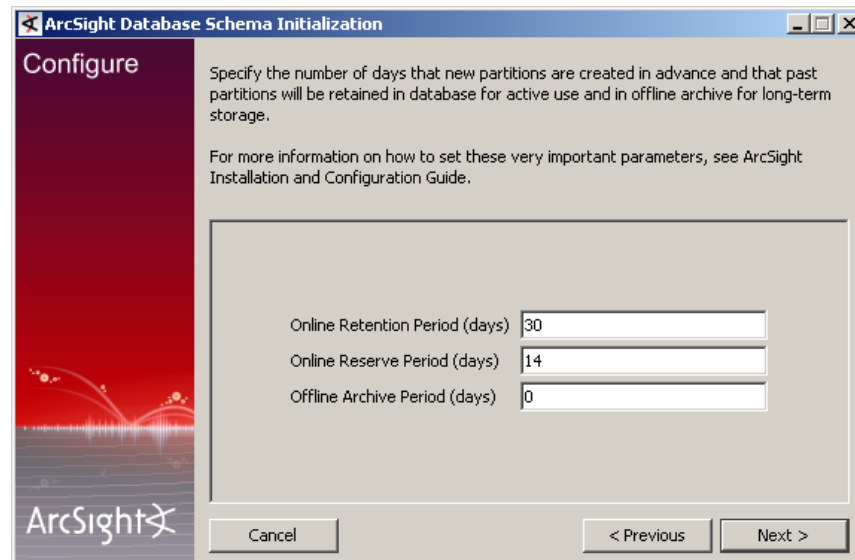


You will see a warning message saying that all existing tablespaces and schema objects will be deleted.



To initialize the database schema, you must specify the parameters in the next few screens. For more information about these parameters, see ["Configuring Partition Management" on page 61](#)

- 11** You will be prompted with the partition retention information. The partitions will be retained in the database for the number of days that you specify in the 'Online Retention Period' field.



The screenshot shows the 'ArcSight Database Schema Initialization' window, 'Configure' tab. The window title bar includes the ArcSight logo and standard window controls. The left sidebar features the ArcSight logo and a red decorative background. The main content area has a title 'Configure' and a description: 'Specify the number of days that new partitions are created in advance and that past partitions will be retained in database for active use and in offline archive for long-term storage. For more information on how to set these very important parameters, see ArcSight Installation and Configuration Guide.' Below this, there are three input fields: 'Online Retention Period (days)' with a value of 30, 'Online Reserve Period (days)' with a value of 14, and 'Offline Archive Period (days)' with a value of 0. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

Configure

Specify the number of days that new partitions are created in advance and that past partitions will be retained in database for active use and in offline archive for long-term storage.

For more information on how to set these very important parameters, see ArcSight Installation and Configuration Guide.

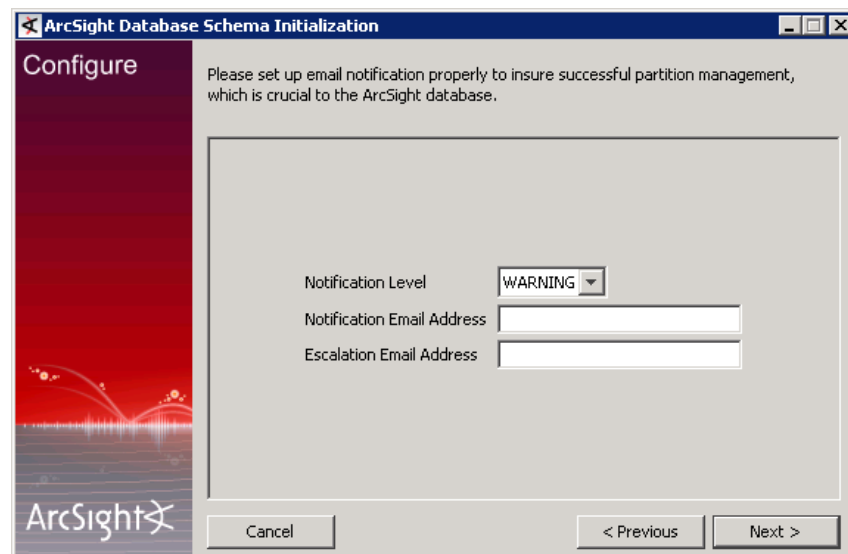
Online Retention Period (days) 30

Online Reserve Period (days) 14

Offline Archive Period (days) 0

Cancel < Previous Next >

- 12** In the next screen enter the e-mail notification to be sent in the event that the Partition Manager encounters a problem.



The screenshot shows the 'ArcSight Database Schema Initialization' window, 'Configure' tab. The window title bar includes the ArcSight logo and standard window controls. The left sidebar features the ArcSight logo and a red decorative background. The main content area has a title 'Configure' and a description: 'Please set up email notification properly to insure successful partition management, which is crucial to the ArcSight database.' Below this, there are three input fields: 'Notification Level' with a dropdown menu showing 'WARNING', 'Notification Email Address', and 'Escalation Email Address'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

Configure

Please set up email notification properly to insure successful partition management, which is crucial to the ArcSight database.

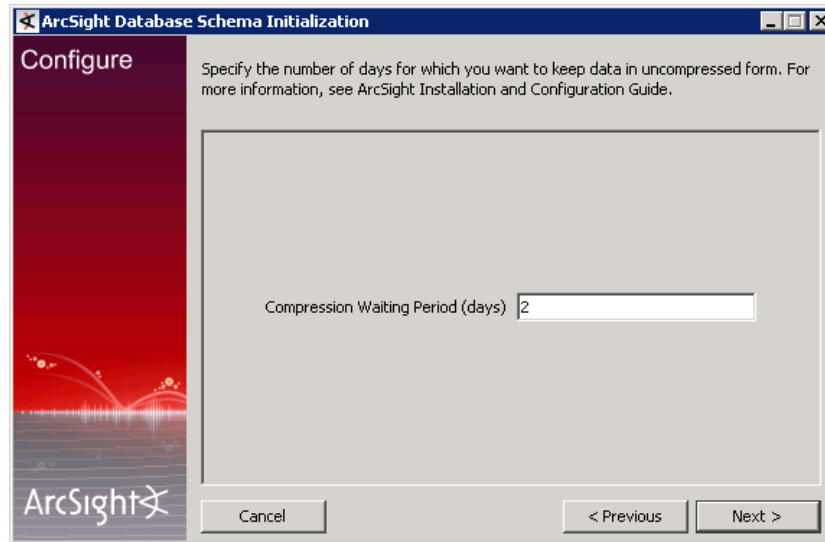
Notification Level WARNING

Notification Email Address

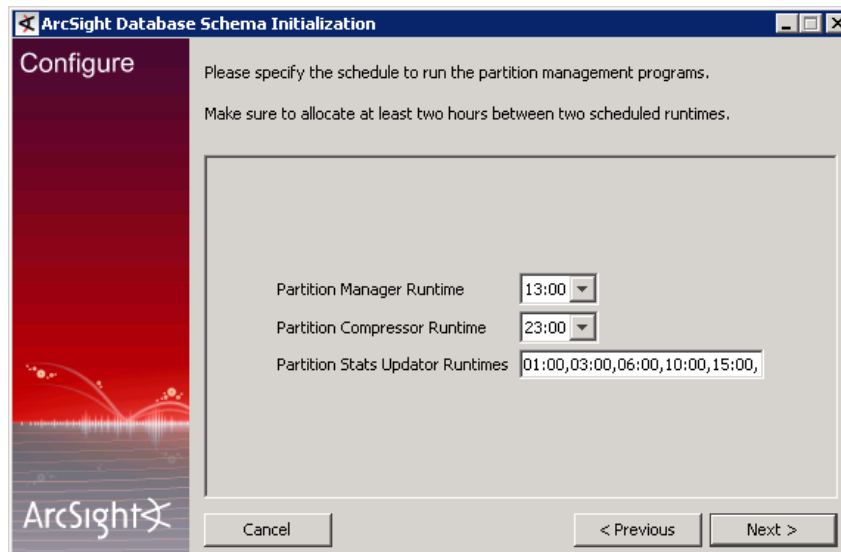
Escalation Email Address

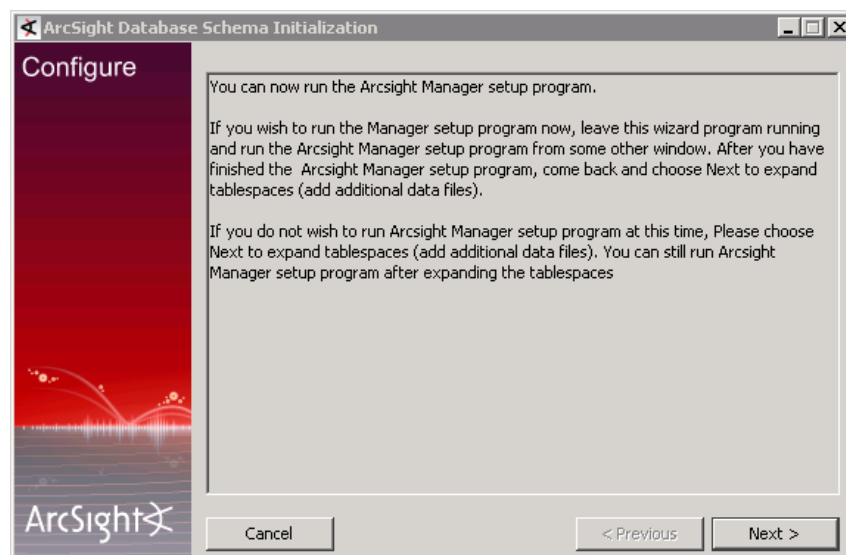
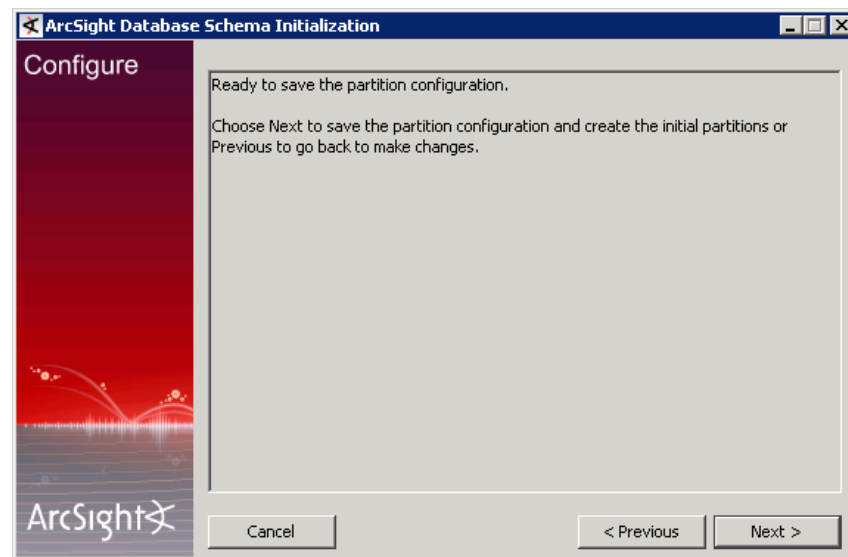
Cancel < Previous Next >

- 13** Enter the number of days that you want to keep the partition in an uncompressed form.

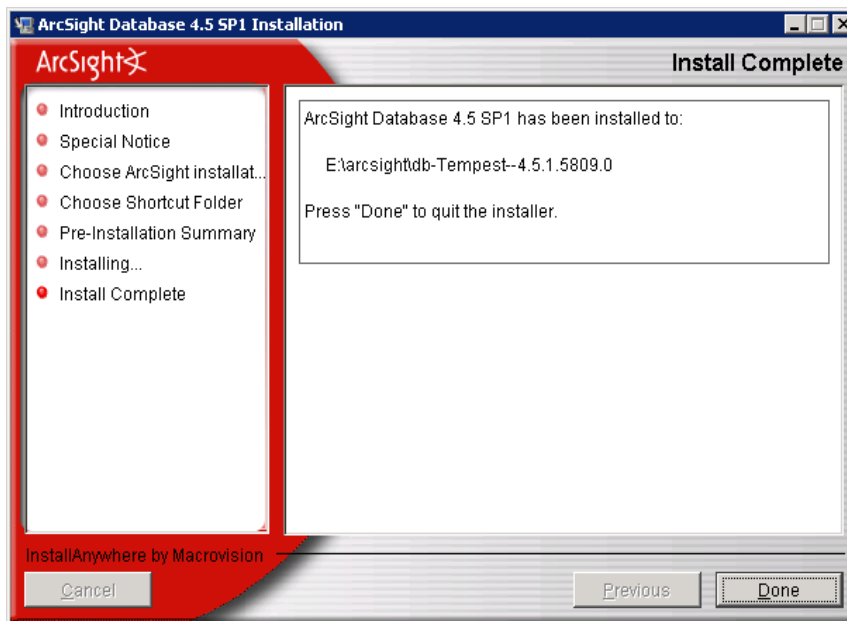
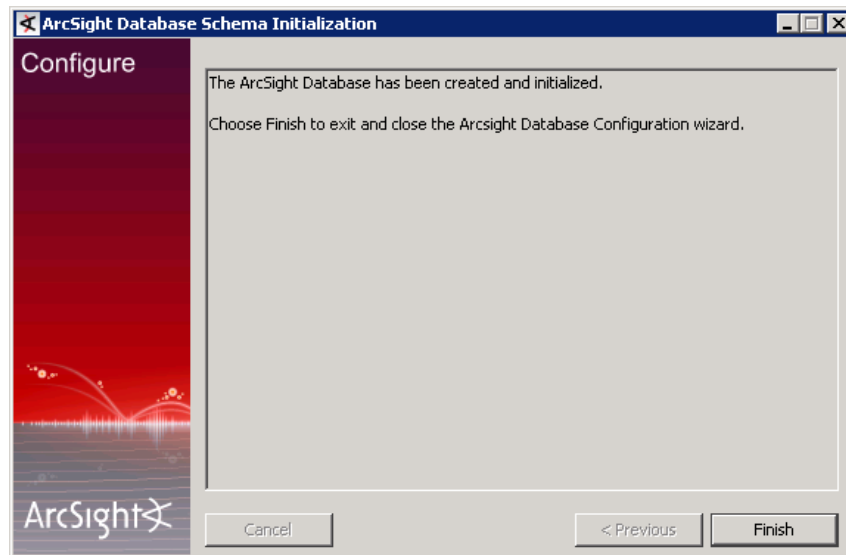


- 14** In the next screen, you will be prompted to schedule the partition management programs. The Partition Manager runs only once in 24 hours, and you can configure that time in the following panel.





You have installed the Oracle 10g database and the ArcSight Database component.



- 15** Make sure to run the following command (while logged in as sysdba) to update the IO transfer speed in the database. If you do not run this script, Oracle defaults to a very low IO transfer speed estimate that adversely affects the query execution plan.

```
% arcdbutil sql
```

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



```
SQL> @ARCSIGHT_HOME\utilities\database\oracle\common\sql\
GatherSystemStats.sql
```



This script should be run every time you make any storage hardware changes that affects IO transfer speeds.

Restarting or Reconfiguring ArcSight Database

If you exit the ArcSight Database Configuration Wizard at any step or need to re-initialize Oracle at a later date, run the following command in `<ARCSIGHT_HOME>\bin` to restart the configuration process:

```
arcsight database init
```

Re-initialization will delete all resource and event data. However, the wizard allows you to avoid recreating the ArcSight Database user account and tablespaces.

Configuring Partition Management



Not all ESM versions or ArcSight Express models support the Partition Archiver.

To improve overall system performance and availability, and to enhance the ease of data management, the ArcSight Database component utilizes several advanced features available in underlying DBMS products (such as Oracle), including table and index partitioning. Table and index partitioning allow large tables and their indexes to be split into individually managed smaller pieces, while retaining a single application-level view of the data.

ArcSight offers advanced life-cycle management facilities for security-event data partitions as an optional feature. This feature fully automates the database partition management process so that partitions containing old event data can be saved in offline archives automatically, and later be easily brought back online so security analysts can conduct forensic analyses using historical data from those archived partitions. This feature offers the ability to dramatically reduce the online storage requirements for the ArcSight Database.

Overview

The ArcSight Database uses partitioned tables for event data with the event end-time column as the partitioning key. By default, these tables are logically divided into daily partitions with midnight (local time) as the partition boundaries.

The following diagram illustrates the overall design for database partition management in the ArcSight Database when partition archiving is enabled.

As the diagram shows, partition archives are first created on online storage devices that are accessible to the database server. Depending on the amount of online storage available, partition archives can remain on the online storage device or be put on removable storage media such as tapes or DVDs. They can be taken offline anytime because archived partitions are no longer part of the database. However, before an archived partition can be

reactivated for historical replays, it must be mounted again on a storage device that is accessible to the database server.

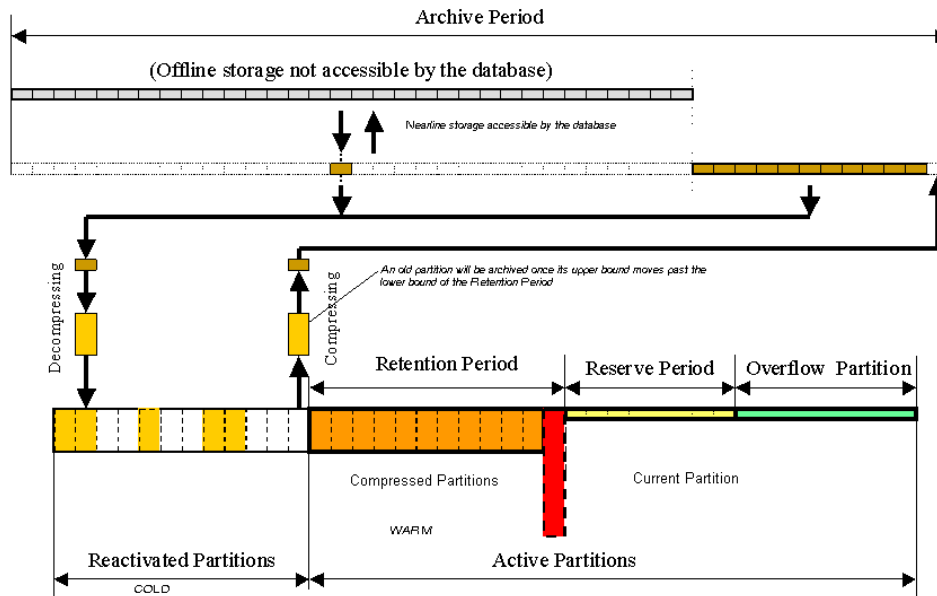


Figure 2-1 ArcSight Database Partition Management (Process View)

The ArcSight Partition Manager, a component in the ArcSight Manager, together with Partition Archiver running on the Database server, manages the life-cycle of partitions, from creation to elimination, as shown in the following state diagram:

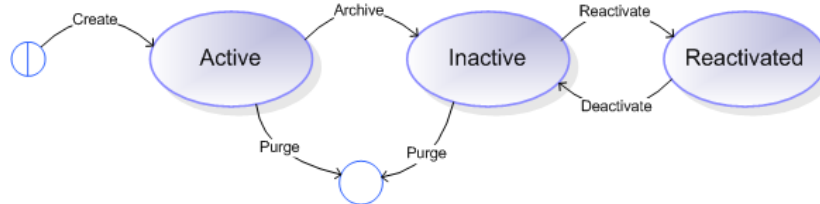


Figure 2-2 Partition state diagram

The database initialization process includes various parameters related to partition management, including the archive period, the retention period, the reserve period, the invocation mode and scheduled runtime for the Partition Manager and, if archiving is enabled, the invocation mode of the Partition Archiver.

During the startup process, based on the current partition management configuration in the database, the ArcSight Manager creates one or more scheduled tasks for the Partition

Manager, the Partition Compressor, the Partition Statistics Updater, and the Partition Archiver.



During the partition archiving process, the Partition Archiver creates some temporary objects which are automatically deleted on the completion of the process. Do not schedule database backups while the partition archiving is in progress in order to avoid these temporary objects from being persisted in your database.

If the Partition Manager is set to run in AUTOMATIC mode, at its scheduled runtime, it performs the appropriate management operations on all active partitions. More specifically, under normal operational conditions, the Partition Manager will:

- Purge the oldest active partition that moves outside of the current Retention Period if the Partition Archiving feature is not enabled;
- Repair the newest reserve partition if its creation process was not fully successful;
- Create a new reserve partition by splitting the current Overflow Partition;

Successful partition management is crucial to database health and performance. Therefore, the Partition Manager should never be disabled for production systems.

Without up-to-date statistics, the query performance of your Oracle database will degrade dramatically. The Partition Statistics Updater will update the statistics for the Current Partition at the times you specify, if it is enabled.

If the Partition Compressor is set to run in AUTOMATIC mode, at its scheduled runtime, it will compress past partitions in the Retention Period that have not been compressed yet and update their statistics once the compression process is completed successfully.

If Partition Archiver is set to run in AUTOMATIC mode, and Partition Archiver is installed and configured properly on the same computer as the database server and it will be running. At its scheduled runtime, Partition Manager will send appropriate archive management commands to Partition Archiver. This process is illustrated by the following diagram:

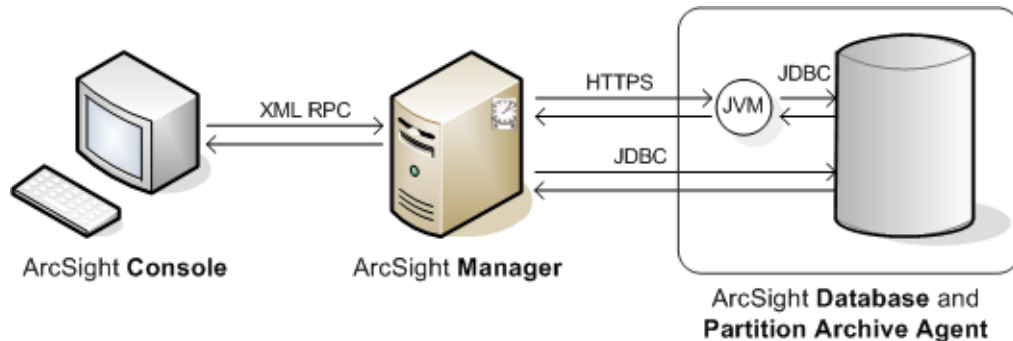


Figure 2-3 Archive management command traffic.

The archive process can also be initiated interactively using the ArcSight Console, providing that the Partition Archiving feature is enabled and set up properly and the user has the appropriate access permissions.

The process of reactivating and deactivating an archived partition is normally initiated manually from an ArcSight Console.

The process of archiving and reactivating a partition may take anywhere from a few minutes to several hours, depending on the size of the partition.

Unlike automatic archiving, the process of reactivating and deactivating an archived partition normally involves some human interaction.

If the archive file for an archived partition is already (or still) available in the archive directory, a user in the ArcSight user group "Administrators" will be authorized to send the reactivation command to the Partition Archiver. If the archive file is stored on removable storage media in an offline location like a tape shelf, the administrative user may have to send a request to a Data Center operator to mount the tape and copy the archive file to the archive directory before he or she can actually reactivate the partition.

If you want to keep the archive file in the Archive Directory after the partition is reactivated successfully, you must set the partition management configuration parameter Archive File Option to KEEP. With the KEEP option, partitions can be reactivated and deactivated any number of times, without requiring human interaction such as copying the archive file from a tape.

Reactivated partitions are deactivated automatically by the Partition Archiver once they move past the Archive Period. Such a partition will then be purged the next time Partition Archiver runs. Normally, once the forensic analysis is completed, an administrative user will manually deactivate a reactivated partition using the ArcSight Console.



Once a Partition Archiver operation--archive, reactivate, or deactivate--completes successfully on a resource, the group of that resource is appropriately changed. For example, when a partition is reactivated, the group is changed from "Inactive Partition" to "Reactivated Partition."

When you initiate a Partition Archiver operation from the Console, check the following to ensure that the operation completes successfully:

- Check Partition Archiver logs on the database machine to ensure that the group change took place.
- Refresh the partition resource in the Console to confirm the new group. (Right-click the resource and select Refresh from the drop-down menu to refresh a resource.)

Do not issue a duplicate command on the same partition while the first operation is still in progress.

The archive file for an archived partition is named in the form of "arc_event_PartitionName.FileExtension", where FileExtension can be "zip" for ZIP (the default archive type), "tar.gz" for GZIP, and "tar.bz2" for BZIP2.

Partition Names are unique date stamps and they are permanent. Never change partition names.

Do not rename the archive files. Archive files must be available in the directory specified by the Archive Directory field in the partition resource before the partition can be reactivated.

Partition Configuration Parameters

Certain Partition Management configuration parameters (such as the Archive Directory) are dynamic. You may change dynamic parameters without restarting the ArcSight Manager, but changes to static parameters will not become effective until the ArcSight Manager is restarted. For example, the Manager must be restarted after changing the configuration to

enable or disable Partition Manager, Compressor, Archiver, or Statistics Updater, or to change their scheduled runtimes, because these parameters are static.

Name	Type	Default Value	Valid Value	More Information
Partition Manager Runtime	Static	13:00	00:30 - 23:30	<ul style="list-style-type: none"> Duration of task: Very Short Initiated by Partition Manager in ArcSight Manager Typically, takes a few seconds to one minute to create a new partition
Retention Period	Dynamic	30 (days)	≥ 2 (See Note 1)	
Reserve Period	Dynamic	14 (days)	≥ 7	
Partition Compressor Runtime	Static	23:00	00:30 - 23:30	<ul style="list-style-type: none"> Duration of task: Long Initiated by Partition Compressor in ArcSight Manager CPU and I/O intensive Typically, takes one to two hours to complete (See Note 2)
Compression Waiting Period	Dynamic	2 (days)	≥ 2	

Name	Type	Default Value	Valid Value	More Information
Partition Stats Updater Runtimes	Static	01:00, 03:00 06:00, 10:00 15:00, 21:00	A comma-separated list of runtimes in the form hours:minutes	<ul style="list-style-type: none"> Duration of task: Increases with each subsequent run Initiated by Partition Statistics Updater in ArcSight Manager CPU intensive Typically takes a few minutes for early runs and up to two hours for late runs (See Note 2)
Partition Stats Update Sample Size	Static	1.0 (percent)	0.01 - 5.0	Specifies the size of the random sample of the rows in a partition
Partition Archiver Mode	Static	DISABLED	AUTOMATIC, DISABLED	
Partition Archiver Runtime	Static	19:00	00:30 - 23:30	<ul style="list-style-type: none"> Duration of task: Long Executed by Partition Archiver on the database machine I/O intensive Typically takes up to two hours (See Note 2)
Archive Period	Dynamic	0 (Days)	>=0	
Archive Type	Dynamic	ZIP - On Windows (see Note 5) GZIP - on UNIX and Linux (See Note 3)	For Windows: ZIP, UNCOMPRESSED For UNIX and Linux: ZIP, GZIP, BZIP2, UNCOMPRESSED (See Note 3)	UNCOMPRESSED, a new option introduced in version 3.5 SP2, leaves the files in the partition uncompressed. See Appendix B, Using UNCOMPRESSED Archive Type, on page 155 .

Name	Type	Default Value	Valid Value	More Information
Archive Directory	Dynamic	None	An existing directory to which the Oracle software owner has write privileges. (See Note 4)	
Archive File Option	Dynamic	KEEP	KEEP, DELETE	Specifies whether to keep or delete the archive file in the Archive Directory after the partition is reactivated successfully
Notification Level	Dynamic	WARNING	INFO, WARNING	Specifies the minimum level for which a notification is generated. If INFO is specified, a notification is generated for all information messages, warnings, and errors. If WARNING is specified, a notification is generated for all warnings and errors.
Notification Email Address	Dynamic	None	Any valid e-mail address, or a comma separated list of e-mail addresses	If the value is set to default, the Error Notification e-mail address configured for ArcSight Manager is used.
Escalation Email Address	Dynamic	None	Any valid e-mail address, or a comma separated list of e-mail addresses	This e-mail address must be different from the one specified for Notification E-mail Address

**Note**

- 1 If you decrease the retention period, Partition Archiver archives all partitions that are now outside of the retention period. Because larger than usual amount of data will be archived at once, ensure that you have enough free space in the archive directory for it before you decrease the retention period.
- 2 Duration depends on partition size, database configuration, and concurrent workload.
- 3 On Solaris, you must install the GNU version of tar and make it the default by either deleting the Solaris version or adding the GNU version of tar ahead of other versions to the PATH variable.

Solaris version of the tar command has a file size limit of 8 GB which prevents Partition Archiver from creating a tar file for partitions larger than 8 GB. Therefore, you must use the GNU version of tar.

The GNU version of tar for Solaris is available at <http://www.sunfreeware.com>.

If you do not want to install the GNU version of tar, select ZIP.

On Linux, GNU tar is available by default. Therefore, you do not need to do anything.
- 4 The Archive Directory must be created in advance and the Oracle software owner user must have full access to this directory. Make sure you have enough space in the file system/volume for this directory. ArcSight recommends that you create the Archive Directory on a separate file system/volume.

Changing Partition Management Configurations

To change Partition Manager configuration parameters, log in to the database machine as the Oracle software owner, go to `<ARCSIGHT_HOME>\bin` and run:

```
arcsight database pc
```

Setting Up Partition Archiver

After the ArcSight Manager is running, you can optionally configure the Partition Archiver on the ArcSight Database host.

This section instructs you on how to set up the Partition Archiver in default mode. To set up the Partition Archiver in FIPS mode, see [Appendix G, Installing ArcSight ESM in FIPS Mode, on page 175](#).

**Note**

If you configure Partition Archiver as a service and later try to start it as a process from the command line, you will get an error saying that the Partition Archiver cannot be started and the `partitionarchiver.log` file cannot be accessed. This happens because when the Partition Archiver starts as a service, the `partitionarchiver.log` file gets created by the root user. But, when you start the Partition Archiver as a process, since you logged in as the oracle user, the `partitionarchiver.log` file gets created by the oracle user.

To work around this, you should change the `partitionarchiver.log` file owner from root to oracle.

You must be logged in as the Oracle software owner (by default, 'oracle' on UNIX and Administrator on Windows) to configure Partition Archiver. The wizard will configure Partition Archiver as a standalone application and register it with the ArcSight Manager.

To configure Partition Archiver:

- 1 From the database `<ARCSIGHT_HOME>\bin`, run the setup program:

```
arcsight agentsetup -w
```

- 2 Select **Run Connector in default mode** when prompted.



Note

If you would like to run the `arcsight database pa` command or the `arcsight database pm` command in the remote mode on a Partition Archiver running in FIPS mode, you will have to run these commands from the Manager's `<ARCSIGHT_HOME>\bin` directory as opposed to the database `bin` directory.

- 3 Enter the Manager's Hostname and Port.
- 4 Enter the name and password for the user that Partition Archiver uses to run.
- 5 Select whether you want to install Partition Archiver as a service.

ArcSight recommends that you install it as a service and do not change the default values unless necessary. Partition Archiver must be run as the Oracle software owner (that is, oracle, by default) on UNIX and as a user (Administrator, by default) on Windows in the local user group ORA_DBA.

To install Partition Archiver as a service on UNIX, log in as root and run the following command:

```
<ARCSIGHT_HOME>/bin/arcsight agentsvc -i -u OracleSoftwareOwner
```

where OracleSoftwareOwner is oracle by default.

If need be, you can re-register Partition Archiver using the following command:

```
<ARCSIGHT_HOME>/bin/arcsight agentsvc -r
```

Then run the command to install it as a service:

```
<ARCSIGHT_HOME>/bin/arcsight agentsvc -i -u OracleSoftwareOwner
```

- 6 Specify the Oracle software owner (.Administrator, by default) and its password. Although you can use another user in the local group ORA_DBA, it is not recommended. Partition Archiver cannot run as the default Local System account.

Starting and Stopping Partition Archiver

To start or stop Partition Archiver as a Windows service, log in as Administrator and use the Windows services applet to start or stop the service.

To start or stop Partition Archiver as a Unix service, log in as root and run:

```
/etc/init.d/arc_oraclepartitionarchiver_db {start|stop}
```



Note

To run Partition Archiver in standalone mode, log in as the Oracle software owner and run:

```
<ARCSIGHT_HOME>/bin/arcsight agents
```

**Note**

On a 32-bit Windows 2003 SP2, if you are installing the Partition Archiver for the first time on this system, you might see this error upon starting the Partition Archiver service:

Could not start the ArcSight Oracle Partition Archiver Database service on local computer.

The service did not start due to a logon failure.

To work around this issue:

- 1 Go to Service control panel.
- 2 Right-click on the **ArcSight Oracle Partition Archiver Database** service.
- 3 Select the **LogOn** tab.
- 4 Make sure that **This account** radio button is selected.
- 5 Enter the user name and password and click **OK**.

Re-registering Partition Archiver with ArcSight Manager

Partition Archiver communicates with the ArcSight Manager using the same infrastructure that the SmartConnectors use. However, unlike SmartConnectors, only one instance of Partition Archiver can be registered with the Manager at any given time. If you try to register Partition Archiver more than once with the same Manager, it will fail.

If you need to re-register Partition Archiver with a Manager, you must first delete the instance that is currently registered with it. Then, follow instructions in [“Setting Up Partition Archiver” on page 68](#).

Deleting the Partition Archiver Service

To delete an existing Partition Archiver service, follow these steps:

- 1 Log in as the Oracle software owner, oracle on UNIX and Administrator on Windows (by default).
- 2 Run this command:

```
<ARCSIGHT_HOME>/bin/arcsight agentsvc -r
```

If the above command fails, you must manually clean up the existing set up using these instructions:

- a Delete the service configuration file as follows:

```
user/agent/default/agent.wrapper.conf
```

- b Delete the service, as follows:

On UNIX, log in as root and run these command:

```
rm /etc/init.d/arc_oraclepartitionarchiver_db
```

```
rm /etc/rc?.d/*arc_oraclepartitionarchiver_db*
```

On Windows, run this command in `<ARCSIGHT_HOME>`:

```
bin\util\win32\ invoker remove arc_oraclepartitionarchiver_db
```

Reinstalling the Partition Archiver Service

To reinstall the Partition Archiver service, follow these steps:

- 1 Log in as the Oracle software owner (by default, oracle on UNIX and Administrator on Windows).
- 2 Run this command:

UNIX: `<ARCSIGHT_HOME>/bin/arcsight agentsvc -i -u oracle`

WINDOWS: `<ARCSIGHT_HOME>\bin\arcsight agentsvc -i -u
.\Administrator -p AdministratorPassword`

Changing the Password for Partition Archiver

Partition Archiver logs in to the ArcSight Database with the same user name and password as the ArcSight Manager uses. If you change the password for the ArcSight Database user, run the command `arcsight database pc` to update the password and restart the Partition Archiver service so that Partition Archiver can continue to log in.

Remember to renew the password for the ArcSight Database user if your company has a database password renewal policy in place. Otherwise, both the ArcSight Manager and Partition Archiver will not be able to log in to the database.

Uninstalling the ArcSight Database Software

Stop ArcSight Database before uninstalling it.

To uninstall on Windows, open the **Start** menu. Run the Uninstall ArcSight Database 4.5 program found under All Programs | ArcSight Database. If a shortcut to the ArcSight Database was not installed on the Start menu, locate the `<ARCSIGHT_HOME>\UninstallerData` folder and double-click:

`Uninstall_ArcSight_DB.exe`

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

`./Uninstall_ArcSight_DB`

The Uninstall utility removes files and folders that were installed during the database installation. It does not remove any files or folders created after the installation, such as log or configuration files. Additionally, this utility only removes the ArcSight components of the database and does not uninstall the Oracle database.



- 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).
- The Uninstaller does not remove all the files and directories under the database home folder. Please delete these folders manually after the uninstallation is complete.

Chapter 3

Installing ArcSight Manager

This chapter describes the installation and configuration of the ArcSight Manager in default mode. To install the Manager in FIPS mode, see [Appendix G, Installing ArcSight ESM in FIPS Mode, on page 175](#). The following topics are covered in this chapter:

[“ArcSight Manager Supported Platforms” on page 73](#)

[“Installing the Manager” on page 74](#)

[“Starting and Stopping the Manager” on page 103](#)

[“Verifying the Manager Installation” on page 103](#)

[“Reconfiguring ArcSight Manager” on page 104](#)

[“Uninstalling ArcSight Manager” on page 106](#)



Note

Do not install the ArcSight Manager unless the ArcSight Database is installed and operating.



Caution

After you have already configured the Manager in either the FIPS mode or the default mode, if you would like to switch the mode, you have to run the Manager setup and choose the mode you want to switch to. For example, if you have already installed your Manager in default mode, and later decide to switch to FIPS mode, you have to run the Manager’s setup program and reconfigure your Manager to run in FIPS mode.

ArcSight Manager Supported Platforms

The following operating system platforms are supported. The sections which follow describe more detailed requirements by platform.



Note

- While single-CPU and single-core systems are not supported, the ArcSight Manager does support multiple-CPU and dual-core systems.
- On 64-bit machines a minimum of 4 GB RAM is required.

Platform	Supported Operating System	Typical System Requirements
Linux	RHEL v4 AS update 8 (32 bit and 64-bit) RHEL v5.3 AS update 2 (32 bit and 64-bit) SUSE Linux 10 SP2 Enterprise Server (64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Microsoft Windows	Microsoft Windows Server 2003 R2 SP2 (32-bit and 64-bit) Microsoft Windows Server 2008 (32-bit and 64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Solaris	Sun Solaris 10 (64-bit)	Sparc-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
IBM AIX	AIX 5L 5.3 (5.3.0.70) 64-bit	Power PC multi-CPU system with 2-16 GB RAM, 2 GB disk space

**Note**

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

The machine hosting the ArcSight Manager should be similar in capacity to the ArcSight Database host, because each will process the same volume of events. More CPUs are desirable for Manager machines, but memory is not as important as it is on Database machines. Disk space for a typical Manager machine might consist of two 72 GB mirrored drives.

The capability of the Manager host platform will determine the number of concurrent Console users and their perceived performance during peak event-per-second episodes. Console performance estimates depend on the number of static viewers compared to more stressful uses such as ad-hoc query and report generation.

Installing the Manager

**Caution**

In some Solaris environments, when upgrading the ESM Manager and also when installing the solution packages, these actions do not complete. This could possibly be due to your Solaris system not meeting the minimum system requirements.

Check ["ArcSight Manager Supported Platforms" on page 73](#) to make sure that your Solaris system meets the minimum system requirements and retry.

**Note**

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

ArcSight Manager requires that a ArcSight Database be installed prior to starting the Manager installation. For optimal performance, ArcSight recommends that you install the Manager on a different host than the database machine.

To install ArcSight Manager, run the self-extracting archive file that is appropriate for your target platform. Insert the ArcSight Installation CD-ROM or go to the directory where the ArcSight Manager Installer is located.

Create an ArcSight user, usually named 'arcsight,' to own the installation. Log in as the ArcSight user before running the Manager Installation Wizard. The ArcSight Manager Installation Wizard for each platform is described in the following table:

Platform	Installation File
Windows	ArcSight-4.5.x.nnnn.y-Manager-Win.exe ArcSight-4.5.x.nnnn.y-Manager-Win64.exe
Linux	ArcSight-4.5.x.nnnn.y-Manager-Linux.bin ArcSight-4.5.x.nnnn.y-Manager-Linux64.bin
Solaris	ArcSight-4.5.x.nnnn.y-Manager-Solaris.bin
AIX	ArcSight-4.5.x.nnnn.y-Manager-AIX.bin

Logon as the ArcSight user and run the installation file to extract and run the ArcSight Manager Installer. To run the graphical user interface version, X-Windows must be installed and properly configured.

The ArcSight Manager installation program provides a summary of the ArcSight Manager installation process and any prerequisite steps you should perform before commencing the installation. The sequential steps of the process are listed on the left side of the wizard and will track your progress. You may click **Cancel** at any time, but the ArcSight Manager will only be usable if you complete the installation wizard successfully. If you need to return to a previous step, it is usually possible to click the **Previous** button to go back and change your entry.

- 1 Read the installation process checklist and click **Next**.
- 2 Read the introduction and click **Next**.
- 3 Read the notice and click **Next**.
- 4 Enter or navigate to the location where you would like to install ArcSight Manager and click **Next**.
- 5 Choose the location where you would like to create a shortcut for the Manager and click **Next**.
- 6 Review the summary in the Pre-Installation screen. If anything is incorrect, click **Previous** to make changes. When you are ready to proceed, click **Install**.

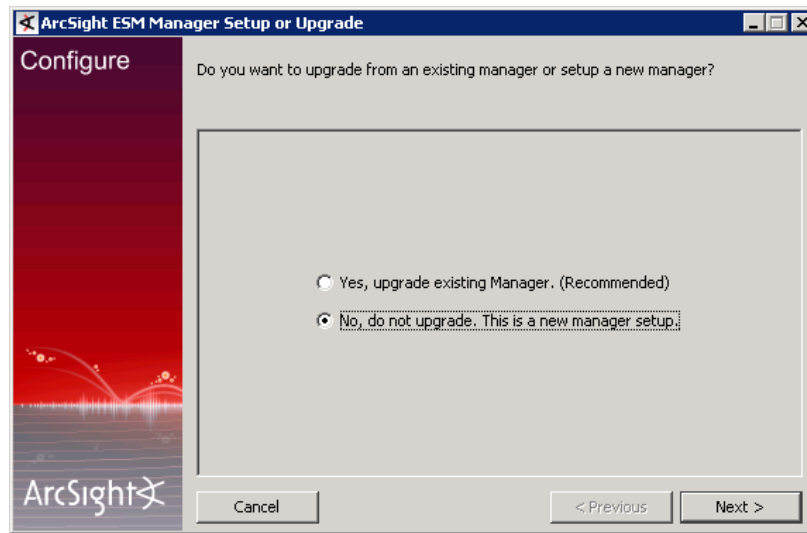
The Installing ArcSight Manager screen appears. It allows you to monitor the installation progress. You may click **Cancel** to quit and install ArcSight Manager at another time.

After the Manager has been installed, you will see the first configuration screen as shown below.



If you are installing in console mode you will have to manually run the setup program by typing `arcsight managersetup` in the installed `<ARCSIGHT_HOME>\bin` directory.

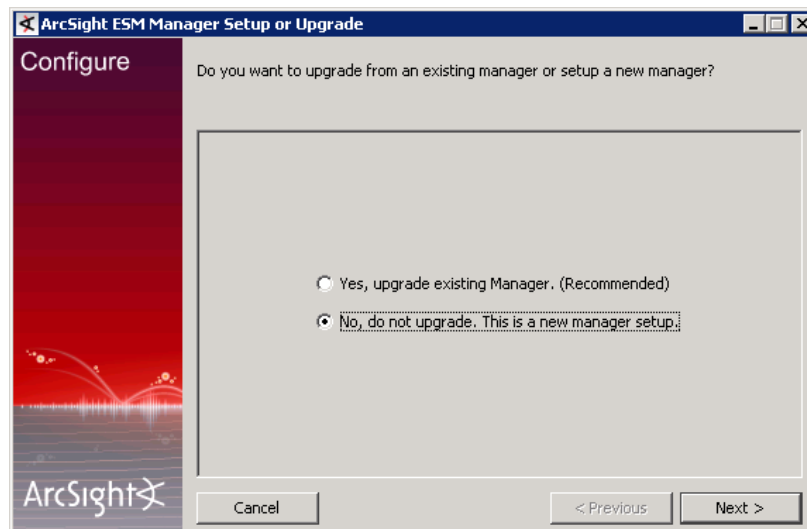
The wizard prompts you to select if you would like to transfer configuration options from a previous installation of ArcSight Manager.



Transferring Configuration from an Existing Installation

If you are installing the Manager in console mode, you will need to run `managersetup` program from the Manager's `bin` directory to start the configuration.

The wizard asks if you would like to transfer configuration options from a previous installation of ArcSight Manager. Since this is a new installation, choose **No, do not upgrade. This is a new Manager setup** to create a new, clean installation and click **Next**.

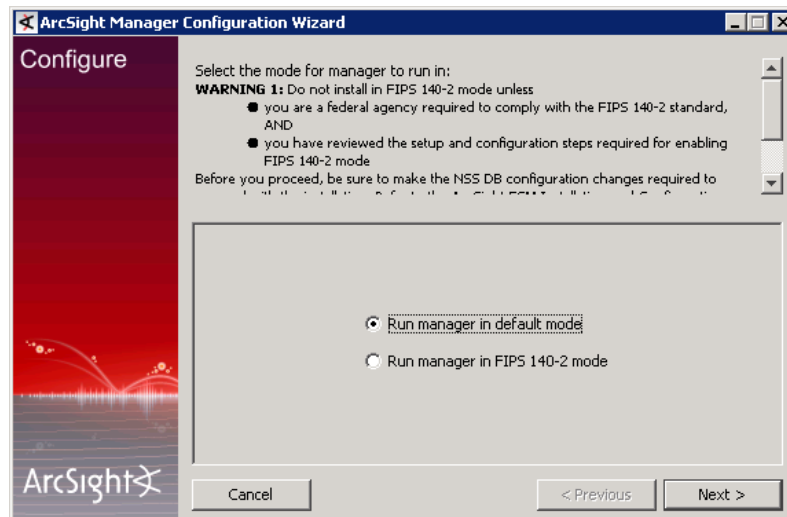


Selecting the Mode in which to Configure ArcSight Manager



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

Next, you will see the following screen:



To configure Manager in Default mode, select the **Run manager in default mode** radio button and click **Next**.

Configuring the Manager's Host Name, Port, and Location

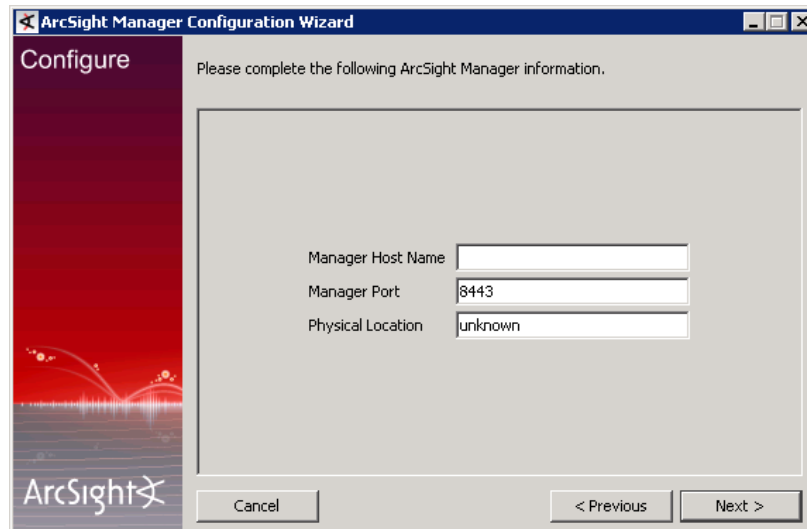
The ArcSight Manager Configuration Wizard establishes parameters required for the Manager to start up on the machine on which it is installed and connect to the ArcSight Database. During configuration, you install license keys and specify notification and e-mail options.



You can re-configure ArcSight Manager at anytime by opening a command window on `<ARCSIGHT_HOME>\bin` and typing the command `arcsight managersetup` within a command prompt window or terminal box.

Parameter	Description
Manager Host Name	Local host name or IP address (or accept the default). Note that this name is what all clients (e.g., ArcSight Console) will need to specify to talk to the ArcSight Manager. Using a host name instead of an IP address is recommended for flexibility. The hostname must match the Common Name of the Manager certificate.
Manager Port	Port number (or accept the default 8443).

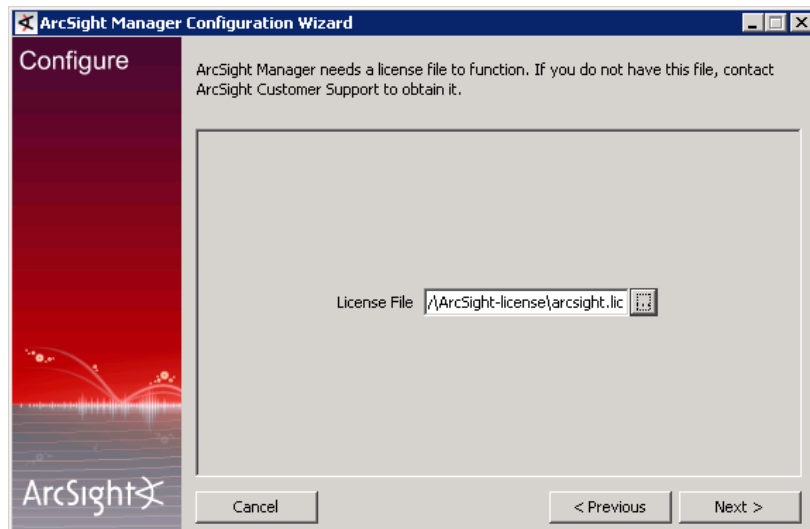
Parameter	Description
Physical Location	Text describing the location of the ArcSight Manager host machine.



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

After entering the ArcSight Manager host information, click **Next**.

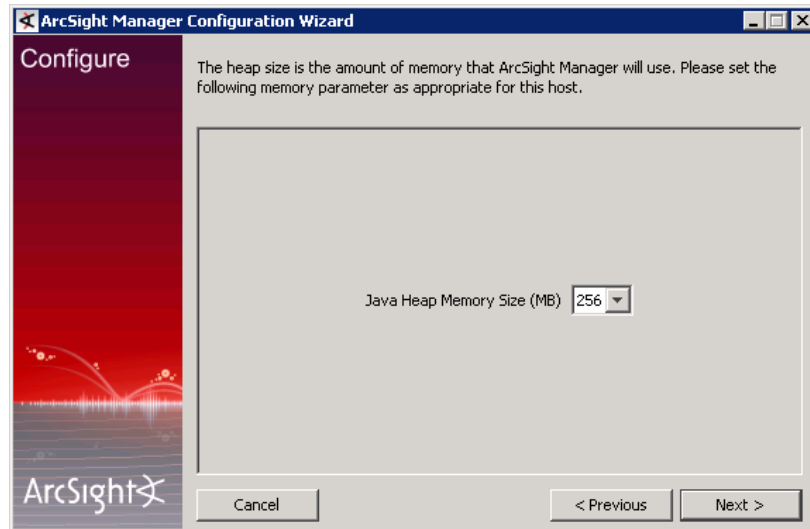
Enter the full path to the `arcsight.lic` file. It will be copied to the appropriate folder by the Configuration Wizard.



The screenshot shows the next 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background with the text 'ArcSight Manager needs a license file to function. If you do not have this file, contact ArcSight Customer Support to obtain it.' Below this is a form with one field: 'License File' with the value '\\ArcSight-license\arcsight.lic'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

Java Heap Memory Size

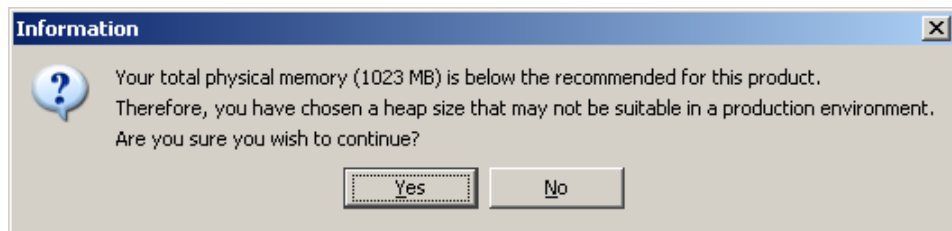
The ArcSight Manager Configuration Wizard prompts you to specify the memory heap size the ArcSight Manager will use.



The heap memory size is the amount of memory that ArcSight will allocate for its heap. (Besides the heap memory, ArcSight Manager uses some additional system memory as well.) The recommended size for production deployments is at least 512 MB. (Smaller amounts will affect performance.) It is important that the amount of physical memory available on the system be significantly larger than the amount of heap allocated for the ArcSight Manager, so that there is additional space available for the operating system and for cache use. For example, systems with 1 GB of physical memory should set the maximum heap size no larger than 512 MB. If you specify a heap size of 1 GB, the system should have at least 1.5 GB of physical memory.

Set the memory parameter for the ArcSight Manager host machine from the Java Heap Memory Size drop-down menu and click **Next**.

If your machine does not have sufficient memory for the Manager, you will see the following message.



SSL Certification Selection

You will be prompted to select the type of SSL certificate you want to use.



Deciding which SSL certificate to select

ArcSight Manager should be installed with a self-signed or a Certificate Authority (CA) signed SSL certificate. Both are equally secure, however, CA-signed scale better. See *ArcSight ESM version 4.5 Administrator's Guide* for detailed information about certificates.

If you plan on using a CA-signed SSL certificate but do not have one, you can use the demo certificate that ArcSight provides to complete the installation. However, ArcSight strongly recommends that you update it with a signed certificate as soon as possible for the following reasons:

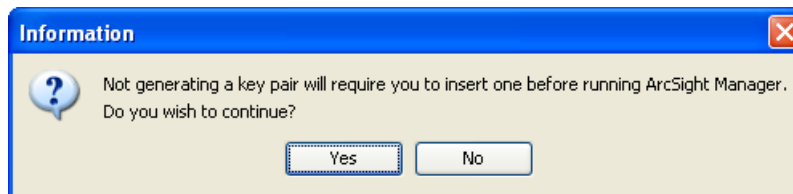
- Demo certificate is not secure. Systems running with this certificate can be easily compromised if attacked.
- When you replace the demo certificate with a signed certificate on the Manager, you have to update the certificate on all Consoles, SmartConnectors, and ArcSight Web servers that communicate with this Manager. This process can be time consuming if you have a large number of SmartConnectors.

For detailed understanding of how SSL is used for communication between ArcSight components, see *ArcSight ESM version 4.5 Administrator's Guide*.

Selecting the SSL certificate

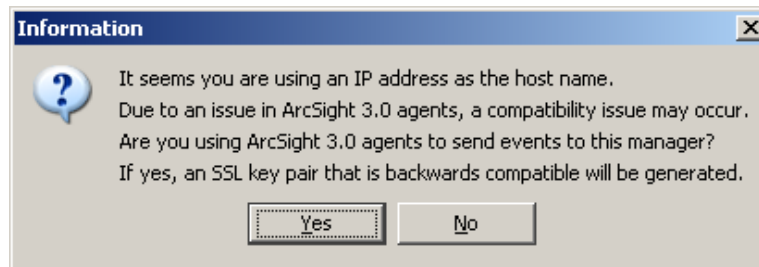
The ArcSight Manager Configuration Wizard prompts you to specify the type of Secured Sockets Layer protocol (SSL) server certificate to use.

To use a CA-signed certificate, select **No key pair**. You will see the following warning:



After completing the Configuration Wizard, follow the procedure described in *ArcSight ESM version 4.5 Administrator's Guide* to install the CA-signed certificate.

To use a self-signed certificate, select **Self-signed key pair**. You will see the following warning:

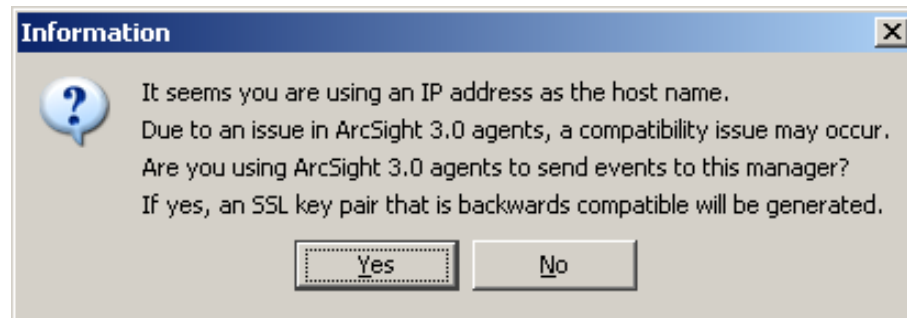


Enter the details of the certificate to be issued:

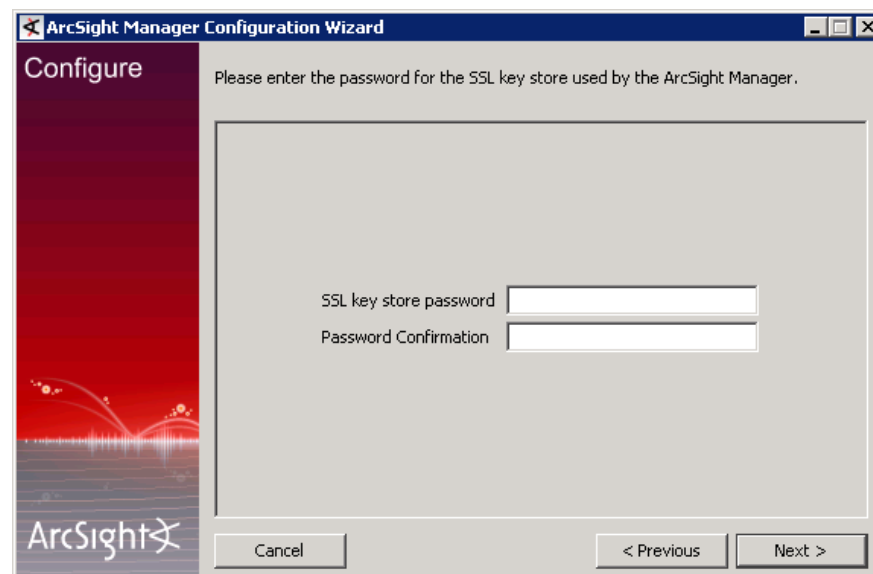
A screenshot of the "ArcSight Manager Configuration Wizard" window, specifically the "Configure" step. The title bar says "ArcSight Manager Configuration Wizard". The left sidebar has a red background with the ArcSight logo at the bottom. The main area has a light gray background and contains the text: "Please complete the following details about the SSL certificate to be issued." Below this text is a form with the following fields: "Validity (days)" with the value "365", "Country", "State", "Locality", "Organization", and "Organizational Unit". At the bottom are three buttons: "Cancel", "< Previous", and "Next >".A screenshot of the "ArcSight Manager Configuration Wizard" window, specifically the "Configure" step. The title bar says "ArcSight Manager Configuration Wizard". The left sidebar has a red background with the ArcSight logo at the bottom. The main area has a light gray background and contains the text: "Please enter the password for the SSL key store used by the ArcSight Manager." Below this text is a form with two fields: "SSL key store password" and "Password Confirmation". At the bottom are three buttons: "Cancel", "< Previous", and "Next >".

Follow the procedure described in *ArcSight ESM version 4.5 Administrator's Guide* to create a self-signed certificate on the Manager.

To use a demo certificate, select **Demo key pair**. You will see the following warning:



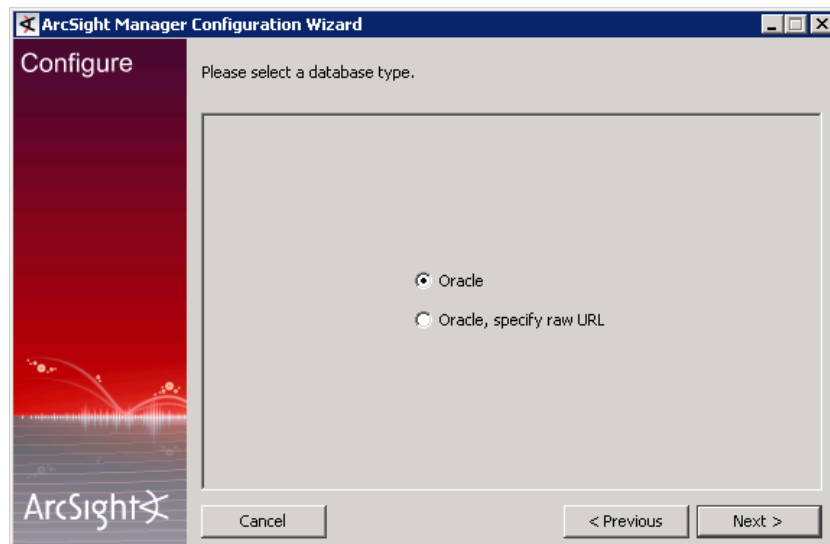
Enter a password for the SSL keystore in the following screen:



After completing the Manager configuration, follow the procedure in *ArcSight ESM version 4.5 Administrator's Guide* to ensure that SmartConnectors, Consoles, and ArcSight Web Servers are configured appropriately for the type of SSL certificate you chose in this step for the Manager.

Database Connection

The ArcSight Manager Configuration Wizard next prompts you to specify the database to which to connect.

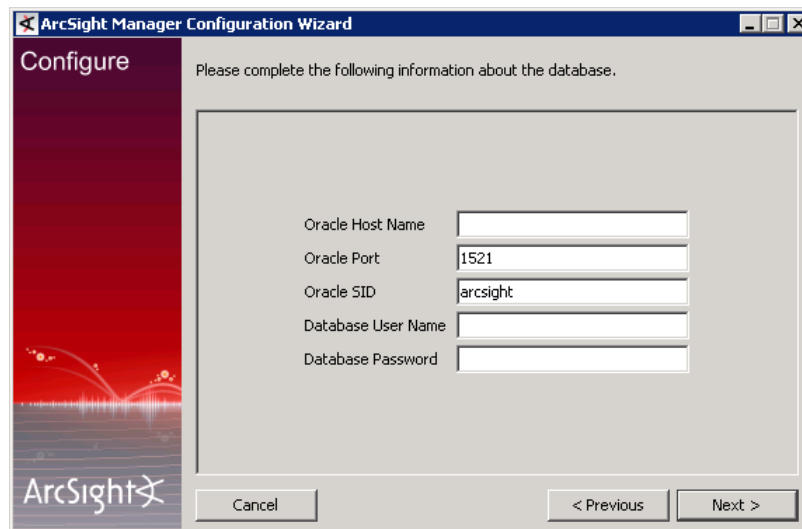


Specify the DBMS on which you installed the ArcSight Database and then click **Next**.

The ArcSight Manager Configuration Wizard next prompts you for information to connect with an ArcSight Database.

The following table describes parameters you need to enter to access the ArcSight Database:

Parameter	Description
Oracle Host Name	Hostname or IP address where the database is installed
Oracle Port	Database communication port
Oracle SID	System identifier for the database
Database User Name	Database user name (same as that specified during ArcSight Database initialization).
Database Password	Database password (same as that specified during ArcSight Database initialization).



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the 'Configure' header and the ArcSight logo at the bottom. The main area has a light gray background with the text 'Please complete the following information about the database.' Below this is a form with five fields: 'Oracle Host Name' (empty), 'Oracle Port' (1521), 'Oracle SID' (arcsight), 'Database User Name' (empty), and 'Database Password' (empty). At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

After specifying the database connection information, click **Next**

Authentication

The Configuration Wizard prompts you to select the type of authentication to use when logging into ArcSight Manager or the ArcSight Console.



Caution

- 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 [Appendix H, Using the PKCS#11 Token, on page 217](#) for details on setting up ESM to use a PKCS #11 token such as the Common Access Card (CAC).

By default, ArcSight ESM 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

ArcSight 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 ArcSight 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.

If a user passes these checks, he/she is authenticated.

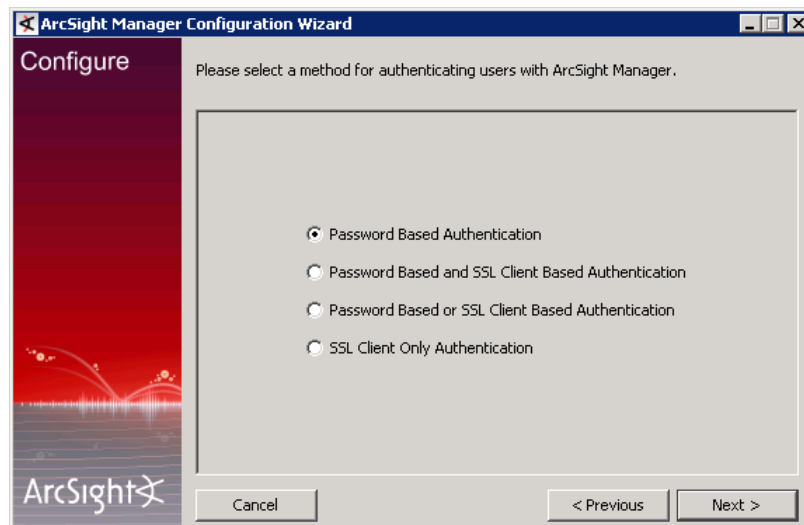
Once you select an external authentication mechanism, all user accounts, including the admin account, are authenticated through it.

Guidelines for setting up external authentication

You must follow these guidelines when setting up an external authentication mechanism:

- All users who will be connecting to the Manager must exist on the Manager.
- All 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.
- All information entered to set up an external authentication mechanism is case insensitive.
- If you need to impose restrictions on the information a user can access, you need to set up Access Control Lists (ACLs) on the Manager.

You will be prompted to select a method for authenticating users.



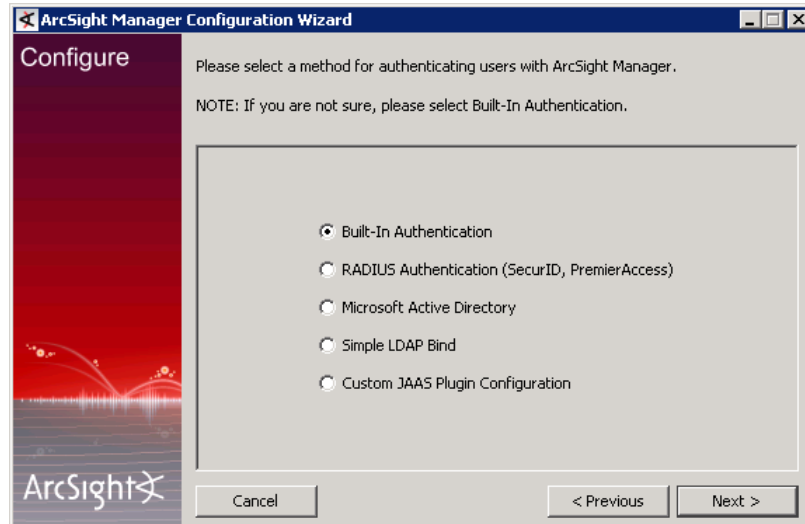
Caution

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

Your authentication will be based upon the User name and Password that you enter when logging into the Console. If you select this option, you will be prompted to select either the ESM built-in authentication or an external authentication method.



Built-In Authentication

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

If you selected this option, go to [“ArcSight Manager Administrator Account Setup”](#) on [page 94](#) section.

Setting up RADIUS Authentication

To configure ArcSight Manager for RADIUS Authentication, choose **RADIUS Authentication** and click **Next**. The next panel prompts you for this information.

The image shows a screenshot of the 'ArcSight Manager Configuration Wizard' window, specifically the 'Configure' step for RADIUS Authentication. The window has a title bar with the ArcSight logo and standard window controls. On the left is a vertical sidebar with the word 'Configure' at the top and the ArcSight logo at the bottom. The main area contains the text 'Please fill out the following information about the RADIUS server.' followed by five input fields: 'Authentication Protocol' (a dropdown menu with 'PAP' selected), 'RADIUS Server Host' (a text box), 'RADIUS Server Type' (a dropdown menu with 'RSA Authentication Manager' selected), 'RADIUS Server Port' (a text box with '1812' entered), and 'RADIUS Shared Secret' (a text box). At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

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. If you want 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: <ul style="list-style-type: none"> • RSA Authentication Manager • Generic RADIUS Server • Safeword PremierAccess
RADIUS Server Port	Specify the port on which the RADIUS server is running.
RADIUS Shared Secret	Specify the RADIUS shared secret string that will be used to verify the authenticity and integrity of the messages exchanged between the Manager and the RADIUS server.



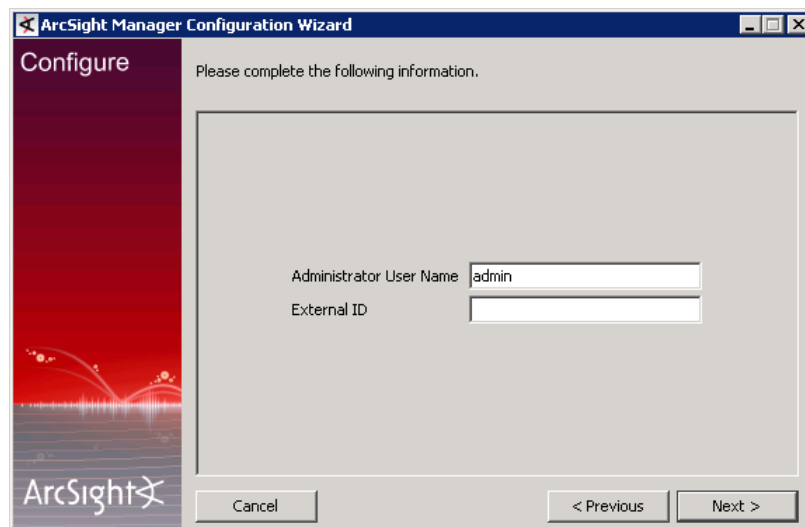
The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar features the ArcSight logo and a red background with a stylized 'X' and the word 'Configure'. The main content area has a light gray background and contains the following text:

Please provide a valid user name and password to test the authentication settings.
NOTE: This account will only be used for the purpose of this test.

Below the text are two input fields:

User Name
User Password

At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.



The screenshot shows the next step in the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar is identical to the previous step. The main content area has a light gray background and contains the following text:

Please complete the following information.

Below the text are two input fields:

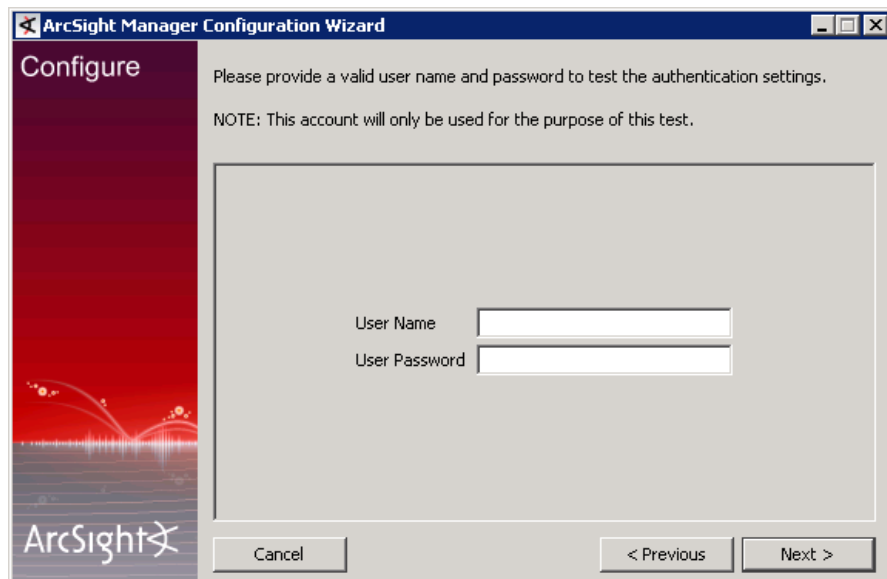
Administrator User Name
External ID

At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

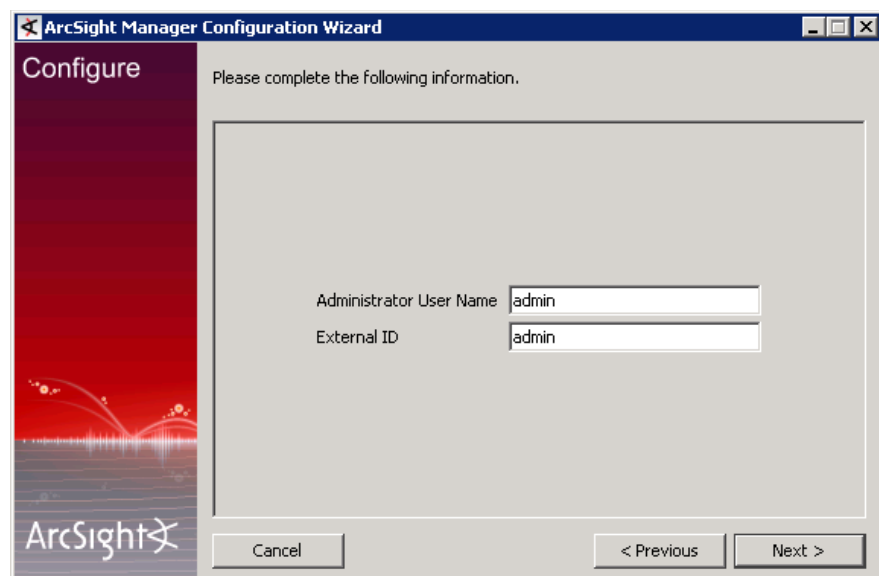
Setting up Active Directory User Authentication

To authenticate users using a Microsoft Active Directory authentication server, choose **Microsoft Active Directory** click **Next**. 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 to use SSL to connect to the Active Directory Server. By default, true (SSL enabled). See "Configuring SSL" on page 90 section for more information.
Active Directory Port	Specify the port on which the Active Directory Server is running.
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.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background. At the top, it says 'Please provide a valid user name and password to test the authentication settings.' followed by a note: 'NOTE: This account will only be used for the purpose of this test.' Below this are two text input fields: 'User Name' and 'User Password'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background. At the top, it says 'Please complete the following information.' Below this are two text input fields: 'Administrator User Name' with the value 'admin' and 'External ID' with the value 'admin'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

Configuring 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`. 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 ArcSight ESM version 4.5 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.

The screenshot shows the 'Configure' panel of the ArcSight Manager Configuration Wizard. The title bar reads 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main content area has a light gray background and contains the following text and fields:

Please fill out the following information about the LDAP server.

LDAP Server

Enable SSL

LDAP Port

At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

Parameter	Description
LDAP Server	Specify the host name of the LDAP Server.
Enable SSL	Whether to use SSL to connect to the LDAP Server. By default, true (enable SSL). See Configuring SSL on Page 84 for more information.
LDAP Port	Specify the port on which the LDAP Server is running. By default, 636.

The screenshot shows the 'Configure' panel of the ArcSight Manager Configuration Wizard. The title bar reads 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main content area has a light gray background and contains the following text and fields:

Please provide a valid user name and password to test the authentication settings.

NOTE: This account will only be used for the purpose of this test.

User Name

User Password

At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

The panel above requires you to 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.

**Note**

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.

ArcSight Manager Configuration Wizard

Configure

Please complete the following information.

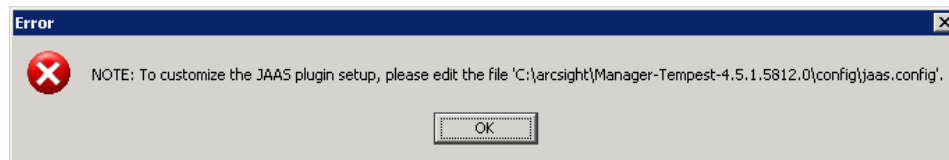
Administrator User Name

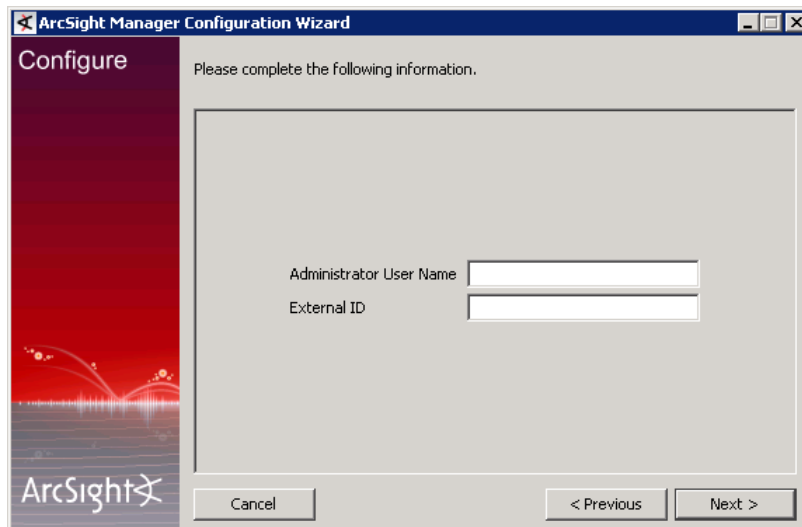
External ID

Cancel < Previous Next >

Using a Custom Authentication Scheme

Choose the **Custom JAAS Plug-in Configuration** option if you want to use an authentication scheme that you have built. You must specify the authentication configuration in a `jaas.config` file stored in the ArcSight Manager `config` directory.





The image shows a screenshot of the 'ArcSight Manager Configuration Wizard' window, specifically the 'Configure' step. The window has a title bar with the text 'ArcSight Manager Configuration Wizard'. On the left side, there is a vertical red bar with the word 'Configure' at the top and the ArcSight logo at the bottom. The main area of the window is light gray and contains the text 'Please complete the following information.' followed by two input fields: 'Administrator User Name' and 'External ID'. At the bottom of the window, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

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 *ArcSight ESM Administrator's Guide* for details on how to do this.

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

ArcSight Manager Administrator Account Setup

The following table describes parameters required to create the administrator account:

Parameter	Description
Administrator User Name	Administrator's user name
External ID	It refers to either the: <ul style="list-style-type: none"> • The CN name used by your PKCS#11 token • Name in the client based SSL certificate • Radius username • Active Directory Login name • LDAP Login name
Administrator Password	Administrator's password
Password Confirmation	Re-enter the password to confirm

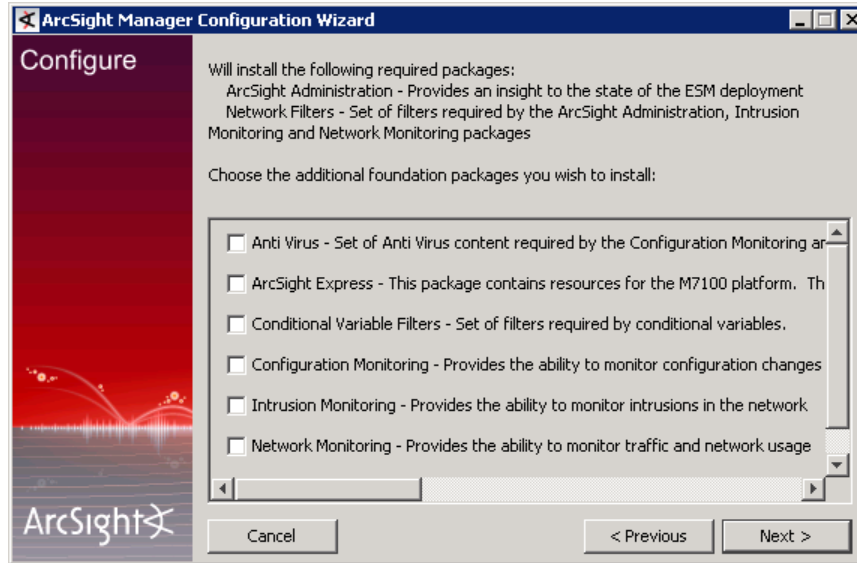
The Administrator user name and password are the user name and password that you will use when you first log in to the ArcSight Console. Using the Console, you can add additional administrators by adding users to the Administrator's group.

When you are finished entering information to create the ArcSight Manager administrator account, click **Next**.

Select Packages

ArcSight System Content is now delivered in the form of packages. System content packages are automatically installed as a part of ArcSight ESM to provide out-of-box resource suites that you can start using immediately to monitor and protect your network.

By default, the ArcSight Administration package that provides you information about your ArcSight ESM installation is installed. You can select other packages to install from the list.



The ArcSight Express content package has been introduced for use with the ArcSight Express appliance. This content is available within the existing foundation packages (as shown in the screenshot above) and need not be installed separately.

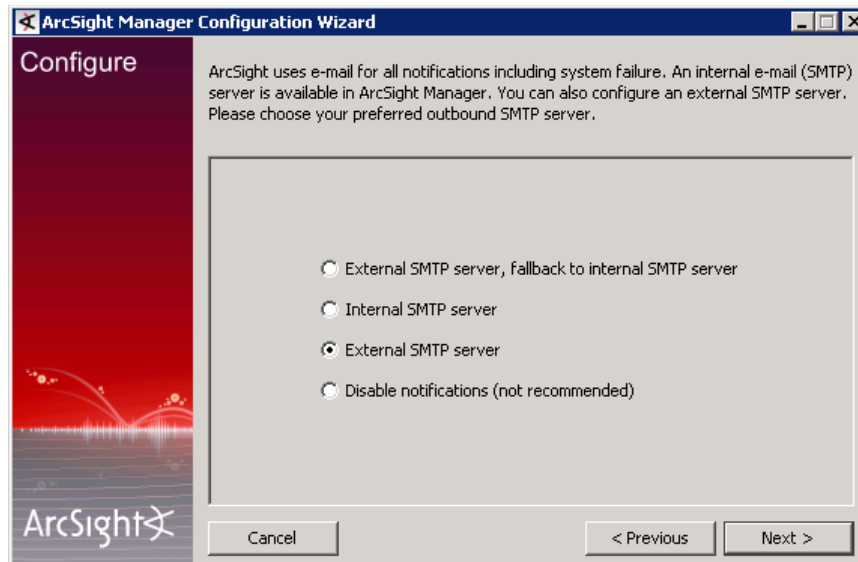
For more information about packages, see the ArcSight ESM *System Content Guide*.

Mail Server

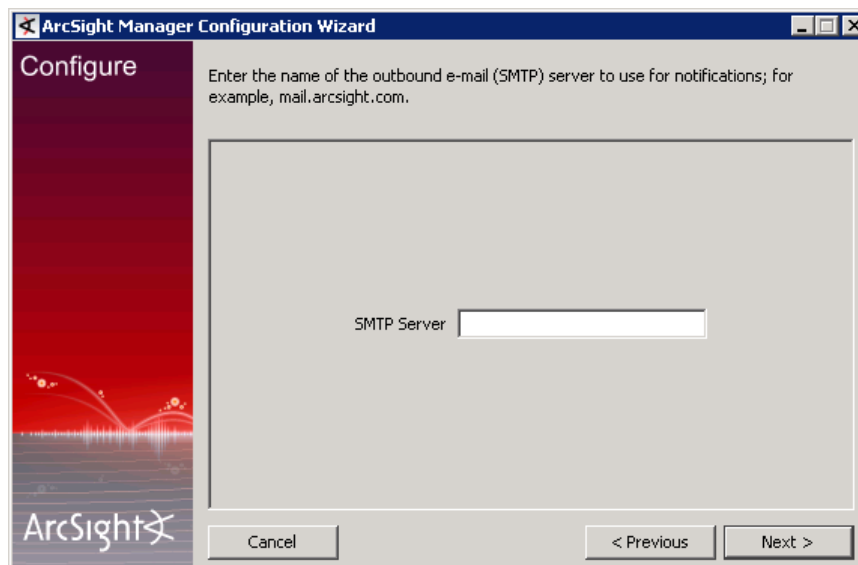


You must set up notification and specify notification recipients in order to receive system warnings. The importance of this step is sometimes overlooked, leading to preventable system failures.

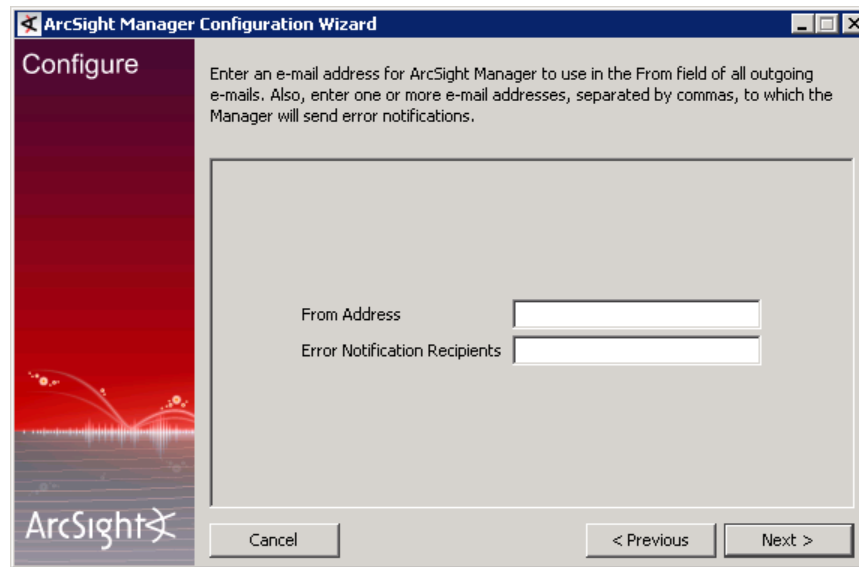
You will be prompted to select a SMTP server:



If you select **External SMTP Server, fallback to internal SMTP server** or **External SMTP server**, you will be prompted to enter the external server name:



You will be also be prompted to enter information to configure the Internal SMTP server.



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background. At the top, it says 'Configure' and provides instructions: 'Enter an e-mail address for ArcSight Manager to use in the From field of all outgoing e-mails. Also, enter one or more e-mail addresses, separated by commas, to which the Manager will send error notifications.' Below this are two text input fields: 'From Address' and 'Error Notification Recipients'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

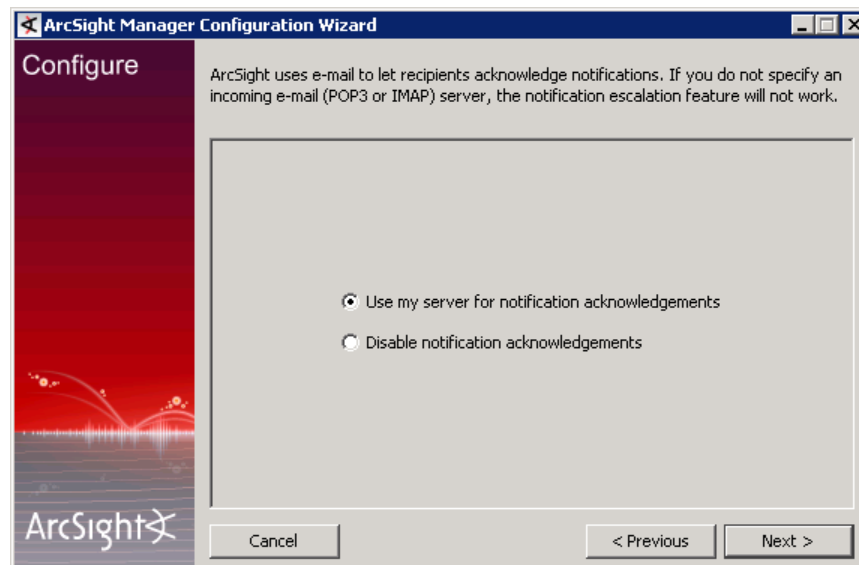
Configure

Enter an e-mail address for ArcSight Manager to use in the From field of all outgoing e-mails. Also, enter one or more e-mail addresses, separated by commas, to which the Manager will send error notifications.

From Address

Error Notification Recipients

Cancel < Previous Next >



The screenshot shows the next 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. On the left is a red sidebar with the ArcSight logo. The main area has a light gray background. At the top, it says 'Configure' and provides instructions: 'ArcSight uses e-mail to let recipients acknowledge notifications. If you do not specify an incoming e-mail (POP3 or IMAP) server, the notification escalation feature will not work.' Below this are two radio button options: 'Use my server for notification acknowledgements' (which is selected) and 'Disable notification acknowledgements'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

Configure

ArcSight uses e-mail to let recipients acknowledge notifications. If you do not specify an incoming e-mail (POP3 or IMAP) server, the notification escalation feature will not work.

☒ Use my server for notification acknowledgements

☐ Disable notification acknowledgements

Cancel < Previous Next >

The following table describes parameters you can enter to set up mail server notification.

Parameter	Description
SMTP Server	The local outgoing Simple Mail Transfer Protocol (SMTP) server host name that is used by the ArcSight Manager to send notification messages
From Address	The e-mail address from where notification messages originate and are sent, appears in the From field of notification messages
Error Notification Recipients	A comma-delimited list of e-mail addresses to notify in case of ArcSight Manager errors that should be directed to an administrator's attention.
Incoming e-mail Server	The Internet Message Access Protocol (IMAP) or Post Office Protocol V3 (POP3) server host name that the ArcSight Manager will use to receive notification confirmations
Server Protocol	Either the IMAP or POP3 protocol used by the ArcSight Manager to communicate with the Incoming Mail Server
User Name	The username that the ArcSight Manager will use to login to the Incoming Mail Server
Password	The password that the ArcSight Manager will use to login to the Incoming Mail Server

The Outgoing Mail Server must be configured to accept and relay e-mail sent from the From Address e-mail address.

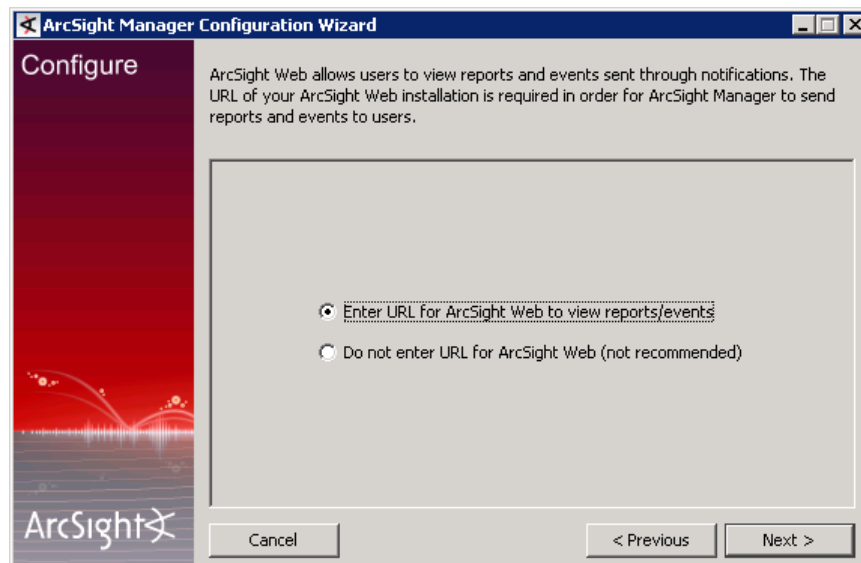
ArcSight Web



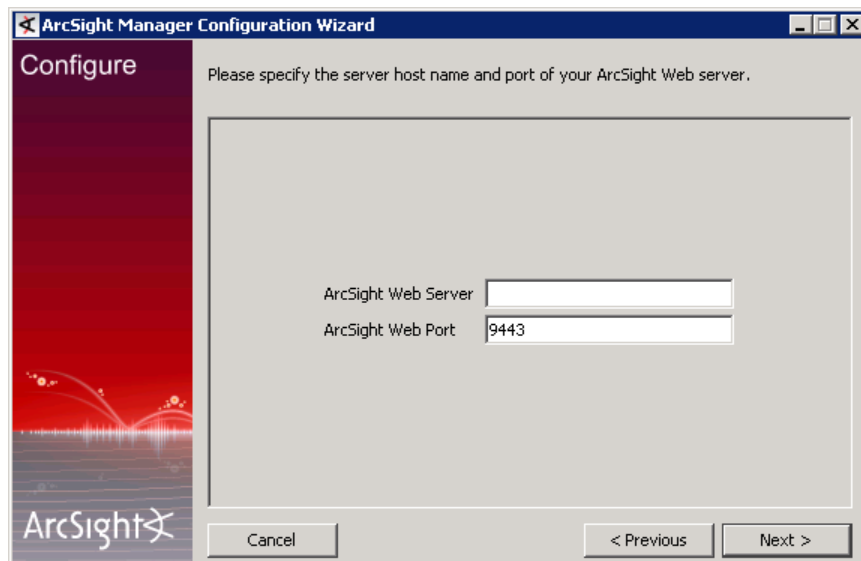
If you choose not to enter a URL for the ArcSight Web at this point, you can do so any time later by issuing the following command from

`<ARCSIGHT_HOME>\bin` directory:

```
arcsight managersetup
```

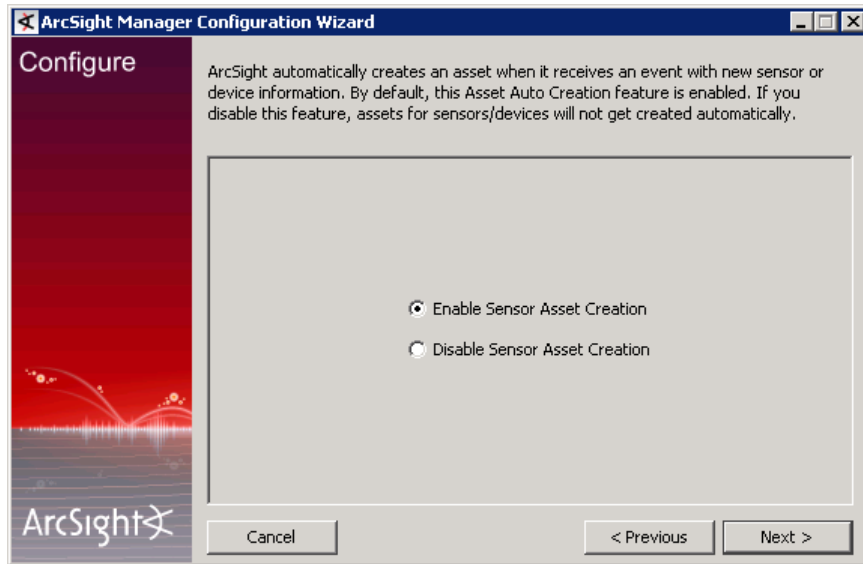


If you chose the **Enter URL for ArcSight Web to view reports/events** option, you will be required to enter the information for the ArcSight Web server:



Asset Auto Creation

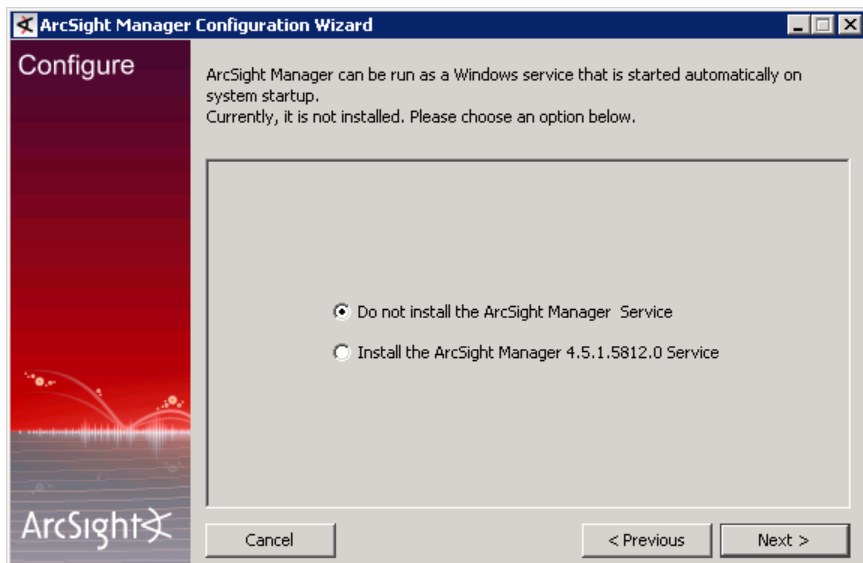
ArcSight Manager can automatically create an asset when it receives an event with a new sensor or device information. By default, assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation**.



Setting up as a Service or Daemon

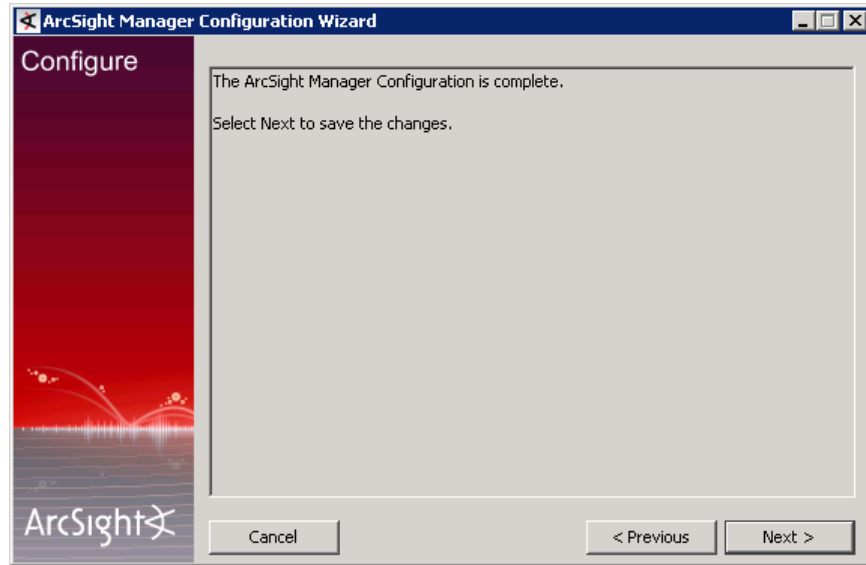
The Configuration Wizard next offers to set up ArcSight Manager as a service (or daemon). Each supported platform provides wizard steps that request platform-specific information—the example shown here illustrates a Windows environment.

Choose whether you want to install the ArcSight Manager as a service, then click **Next**.

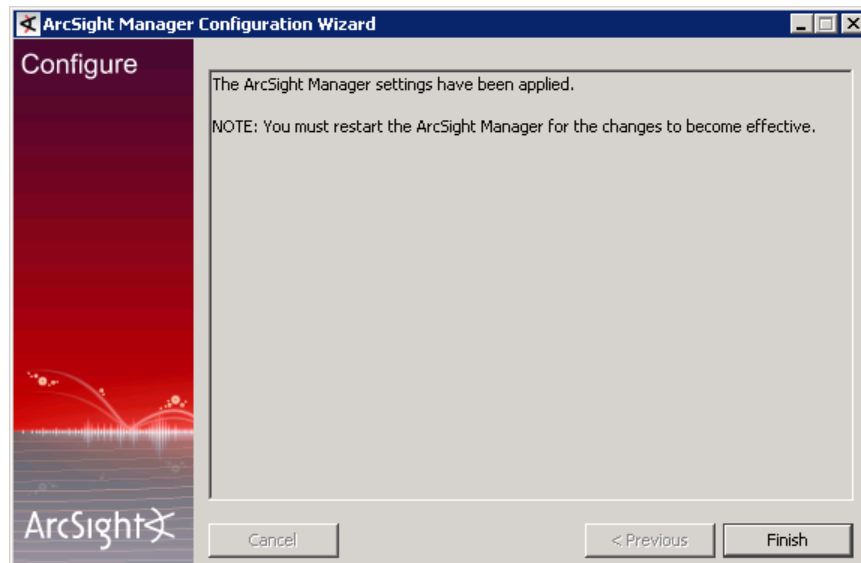


If you choose the option to install ArcSight Manager as a service, the installer prompts you to specify parameters used to set up the service. If you choose not to install ArcSight Manager as a service, you can change the startup configuration later. For more information, see [“Running the Manager as a Service” on page 103](#).

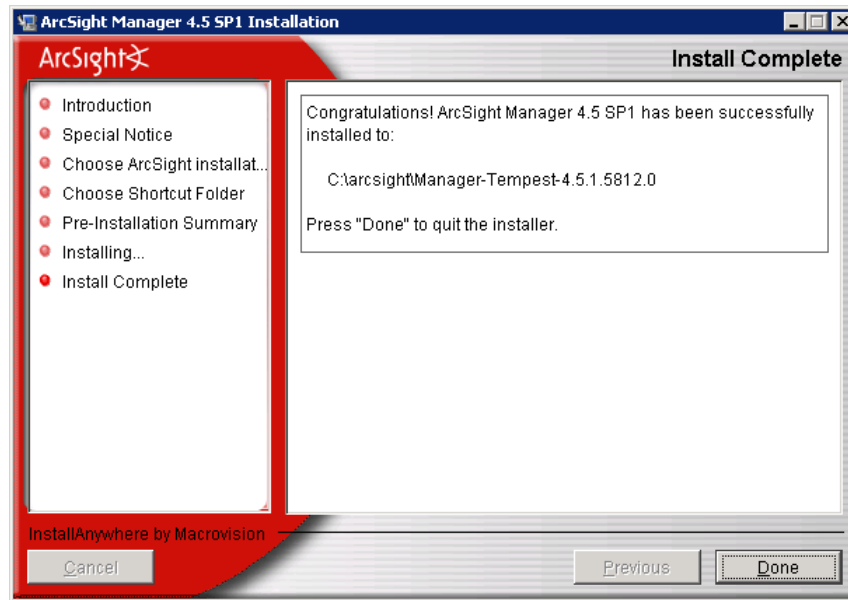
The Configuration Wizard returns a message indicating the ArcSight Manager configuration is complete. Click **Next**.



When ArcSight Manager settings have been applied, click **Finish**.



After installation is complete, you will see the following message.



You can start ArcSight Manager now.



Note

After installing the ArcSight Manager, configure your system's default file permissions so that files created by ArcSight (events, log files, and so on) will be reasonably secure.

On Unix systems, file permissions are typically set by adding the `umask` command to your shell profile. A `umask` setting of 077, for example, would deny read or write file access to any but the current user. A `umask` setting of 000 creates an unnecessary security hole.

Additionally, if you installed the Manager on a SuSE Linux 10 system, you can remove the file called "strings" that you created in the `\sbin` directory.



Note

Chip multi-threading (CMT) machines running Solaris can appear to have more processors than they do and cause the Manager to miscalculate. CMT machine Chip multi-threading (CMT) machines running Solaris can appear to have more processors than they do and cause the Manager to miscalculate. CMT machines require manual configuration to achieve optimal performances require manual configuration to achieve optimal performance.

On Sun Niagara (T1000 or T2000) or other CMT machines, edit the `server.properties` file to change the `queue.start-of-flow.threads` property as follows:

Number of cores	<code>queue.start-of-flow.threads</code>
4	2
6	3
8	4

Note that setting this property will not affect functionality, but could affect system performance.

Starting and Stopping the Manager

Starting the Manager

To start ArcSight Manager from the command line, if it is not configured to run either as a daemon or a service:

- 1 Open a command window or terminal box.
- 2 Change directories to the ArcSight Manager's `<ARCSIGHT_HOME>\bin` directory:
- 3 Type in the following line and press Enter:

```
arcsight manager
```

When you start up, the Manager will display a stream of messages in the command window or terminal box to reflect its status. The command window or terminal box will say Ready when the Manager has started successfully. If you are starting the Manager as a service you can monitor whether or not it has successfully loaded by viewing the `server.std.log` file located in `<ARCSIGHT_HOME>\logs\default`. For example, you could use the command:

```
cd ARCSIGHT_HOME;tail -f logs\default\server.std.log
```

Stopping the Manually Started Manager

To initiate a controlled and graceful shutdown of the ArcSight Manager, open a separate command prompt window and issue the following command:

```
arcsight managerstop
```

Running the Manager as a Service

Use the `managersetup` wizard to run the Manager as a service. When you have finished setup, ArcSight Manager can be controlled via `/etc/init.d/arcsight_manager start|stop`, following the standard method of starting daemon services in Unix. There is also a configuration file `/etc/arcsight/arcsight_manager.conf` that you may change to reflect the location of the ArcSight Manager installation directory and other settings. In addition, the `/etc/init.d/arcsight` scripts will be hooked into the Unix startup procedure, making the ArcSight Manager start and shut down in lock step with the host OS.

Once everything is configured properly, test your configuration setup the next time you start the ArcSight Manager using `/etc/init.d/arcsight_manager start`.

Be sure to start ArcSight Manager this way at least once before relying upon it to start correctly during system boot or startup.

Script output will go to `<ARCSIGHT_HOME>/logs/default/server.script.log`. The `stdout` output of the ArcSight Manager will go to `<ARCSIGHT_HOME>/logs/default/server.std.log`. Run `tail` on these two files to identify any problems causing failures on startup.

Verifying the Manager Installation

The ArcSight Manager displays "Ready" (in the command window and in the log) when it has fully initialized and is ready to respond to communications.

Manager logs are written to `<ARCSIGHT_HOME>\logs\default`.

Reconfiguring ArcSight Manager

To reconfigure ArcSight Manager settings made during installation, shutdown the Manager and then run the ArcSight Manager Configuration Wizard by typing the following command in a terminal box or command prompt window from the Manager's

<ARCSIGHT_HOME>\bin directory:

```
arcsight managersetup
```

The `managersetup` command opens the ArcSight Manager Configuration Wizard.

To change advanced configuration settings (i.e., port numbers, database settings, log location, and so forth) after the initial installation, make changes to the <ARCSIGHT_HOME>\config\server.properties file. ArcSight's default settings are listed in the server.defaults.properties file. You can override these default settings by adding the applicable lines from server.defaults.properties to the server.properties file. These files are located in <ARCSIGHT_HOME>\config.



Note

Never change the server.defaults.properties file. Instead, override individual settings by changing the server.properties file. That way, the original defaults will always be available.

Securing the ArcSight Manager Properties File

The ArcSight Manager's server.properties file contains sensitive information such as database passwords, keystore passwords, and so forth. Someone accessing the information in this file can do a number of things including tampering with the database and acting as a pseudo ArcSight Manager. As a result, the server.properties file must be protected so that only the user account under which the ArcSight Manager is running is able to read it. This can be accomplished by issuing a `chmod` command in Unix and Linux, for example:

```
chmod 600 server.properties
```

This operation is handled during the ArcSight Manager installation. As a result, only the owner of the file (which must be the user that runs the ArcSight Manager) may read or write to the file. For all other users, access to the file is denied.

Sending Events as SNMP Traps

ArcSight provides a filter to send a sub-stream of all incoming events (including rule-generated meta-events) to a specified target using the Simple Network Management Protocol (SNMP). ArcSight's correlation capabilities can be used to synthesize network management events that can then be routed to your enterprise network management console.



Note

By default, snmp.mib.version is set to 2.5. If you cannot find certain fields in the default MIB, change the snmp.mib.version setting to 3.0 in the server.properties file.

To Configure the SNMP Trap Sender

- 1 Copy the SNMP template lines from the default properties file at:

```
<ARCSIGHT_HOME>\config\server.default.properties
```

Uncomment the SNMP lines and save them to your properties file at:

```
<ARCSIGHT_HOME>\config\server.properties
```

Create the `server.properties` file if necessary. Always treat `server.default.properties` as read-only.

- 2 Edit the specific parameters for your situation. The major parameters are described below.
- 3 Restart the Manager for the new settings to take effect.

A description of specific SNMP configuration parameters follows:

```
snmp.trapsender.enabled=true
```

Set this property to `true` in order to enable the SNMP trap sender.

```
snmp.trapsender.uri=/All Filters/ArcSight System/SNMP
Forwarding/SNMP Trap Sender
```

The URI of the zone that is used to decide whether or not an event is forwarded. You can override the zone specified here by changing the zone in the ArcSight Console. Changes to the zone will affect the SNMP trap sender immediately. By default, the SNMP Trap Sender zone logic is: `inZone(Correlated Events)`—that is, only rule-generated meta-events will be forwarded.

```
snmp.destination.host=
```

```
snmp.destination.port=
```

The host name and port number of the SNMP listener must be specified.

```
snmp.read.community=public
```

```
snmp.write.community=public
```

The SNMP community strings must match the community of the receiving host. (The read community is reserved for future use.) The community you must specify will depend on the deployment environment and on the receiving device. Consult the receiving device's documentation to determine the correct community string.

```
snmp.version=1
```

The SNMP version. SNMP versions 1, 2, and 3 supported. For SNMP version 1, set the value for the above property to `0`; for SNMP version 2, set the value for the above property to `1`; and for SNMP version 3, set the value to `3`.

```
snmp.fields=\
```

```
event.eventId,\
```

```
event.name,\
```

```
event.deviceEventCategory,\
```

```
event.type,\
```

```
event.baseEventCount,\
```

```
event.categoryTechnique,\
```

```
event.agentSeverity,\
event.transportProtocol,\
event.attackerAddress,\
event.targetAddress
```

The `snmp.fields` property lists the event attributes to be included in the trap. The syntax follows the ArcSight SmartConnector SDK format. All ArcSight fields can be sent. Note that the identifiers are case-sensitive, do not contain spaces, and must be capitalized except for the first character. For example:

ArcSight Field	SDK/SNMP Trap Sender Identifier
Event Name	eventName
Device Severity	deviceSeverity
Service	Service

The following table illustrates the mapping between ArcSight field types and SNMP field types:

ArcSight Field Type	SNMP Field Type
STRING	OCTET STRING
INTEGER	INTEGER32
Address	IP ADDRESS
LONG	OCTET STRING
BYTE	INTEGER

Additional data values are accessible by name. For example:

```
snmp.fields=event.eventName,additionaldata.myvalue
```

This will send the Event Name field and the value of 'myvalue' in the additional data list part of the SNMP trap. Only the STRING data type is supported for additional data—all additional data values will be sent as OCTET STRING.

Uninstalling ArcSight Manager

Stop ArcSight Manager before uninstalling it.

To uninstall on Windows, open the **Start** menu. Run the Uninstall ArcSight Manager 4.5 program found under All Programs | ArcSight Manager. If a shortcut to the Manager was not installed on the Start menu, locate the `<ARCSIGHT_HOME>\UninstallerData` folder and double-click:

```
Uninstall_ArcSight_Manager.exe
```

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

`./Uninstall_ArcSight_Manager`



- The UninstallerData directory contains a file `.com.zerog.registry.xml` with Read, Write, and Execute permissions for everyone. You can change the permissions to Read and Write for everyone (that is, 666).
 - The Uninstaller does not remove all the files and directories under the ArcSight Manager home folder. Please delete these folders manually after the uninstallation is complete.
-

Chapter 4

Installing ArcSight Console

The ArcSight Console provides a host-based interface (as opposed to the browser-based interface of ArcSight Web) to ArcSight ESM. This chapter explains how to install and configure the ArcSight Console in default mode. To install the Console in FIPS mode, see [Appendix G, Installing ArcSight ESM in FIPS Mode, on page 175](#).

The following topics are covered in this chapter:

- ["Console Platforms" on page 109](#)
- ["Using a PKCS#11 Token" on page 110](#)
- ["Installing the Console" on page 111](#)
- ["Starting the ArcSight Console" on page 124](#)
- ["Reconnecting to the ArcSight Manager" on page 126](#)
- ["Reconfiguring the ArcSight Console" on page 126](#)
- ["Uninstalling the ArcSight Console" on page 127](#)

Install and test the ArcSight Database and Manager before installing the ArcSight Console. The ArcSight Console may be installed on the same host as the Manager, or on a different machine entirely. Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager and Database hosts.

Console Platforms

The following operating system platforms are supported. The sections which follow describe more detailed requirements by platform.



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	RHEL 4.0 WS update 8 (32-bit) RHEL 4.0 AS update 8 (64-bit) RHEL 5.3 Desktop (32-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.

Platform	Supported Operating System	Typical System Requirements
Solaris	Sun Solaris 10 SPARC (64-bit)	Sparc-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Windows	Windows Server 2003, R2 SP2 (32-bit & 64-bit) Windows Server 2008 (64-bit) Windows Vista SP1 (32-bit & 64-bit) Windows XP Professional SP3, 32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM, 2 GB disk space.
Macintosh OS X PPC 10.5 (64-bit)	Macintosh OS X PPC 10.5.6 (64-bit)	

Using a PKCS#11 Token



For this release, the use of PKCS#11 token is supported on Windows XP platform only.

Starting ESM v4.0 SP2, 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. PKCS#11 is a public key cryptography standard which defines an API to cryptographic tokens.

You can use the PKCS#11 token regardless of the mode that the client is running in - with clients running in FIPS 140-2 mode or with clients running in the default mode. See [Appendix H, Using the PKCS#11 Token, on page 217](#) for details on using a PKCS #11 token with the Console.

Installing the Console



Caution

Tools that require a remote login to a Manager running in FIPS mode will need to be run from the Manager's `<ARCSIGHT_HOME>` as opposed to the database's `<ARCSIGHT_HOME>`. However, running these tools in a standalone mode by stopping the Manager and running the tools directly on the database is supported.



Caution

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.



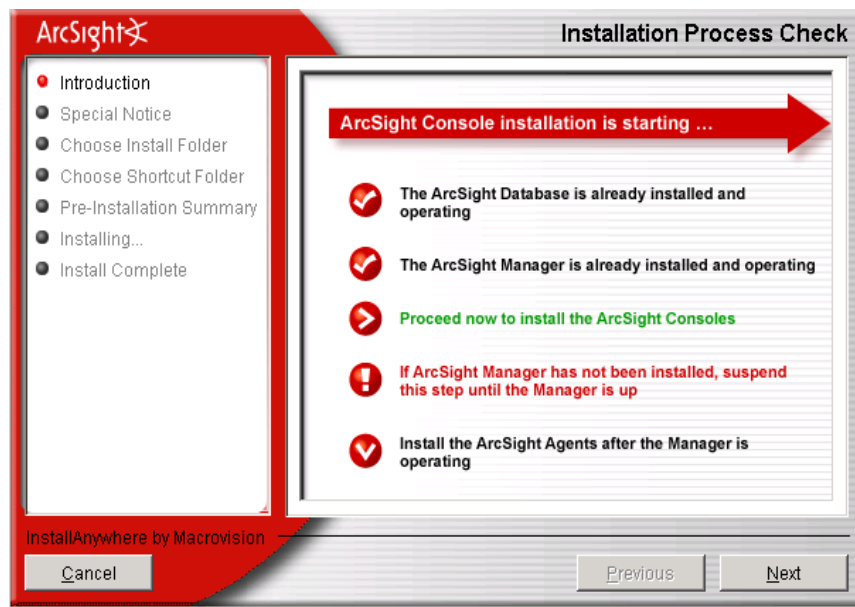
Note

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

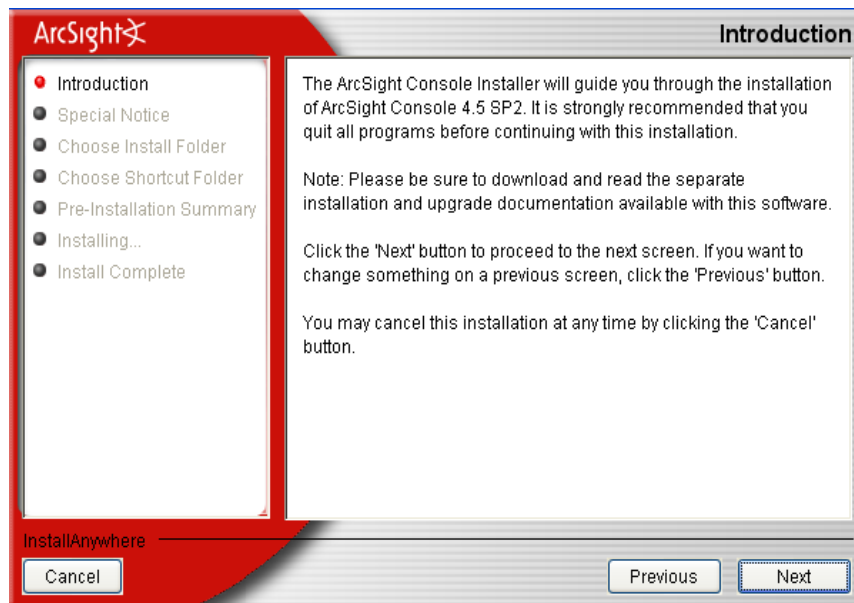
Make sure that you have the ArcSight Manager installed before installing the ArcSight Console.

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.

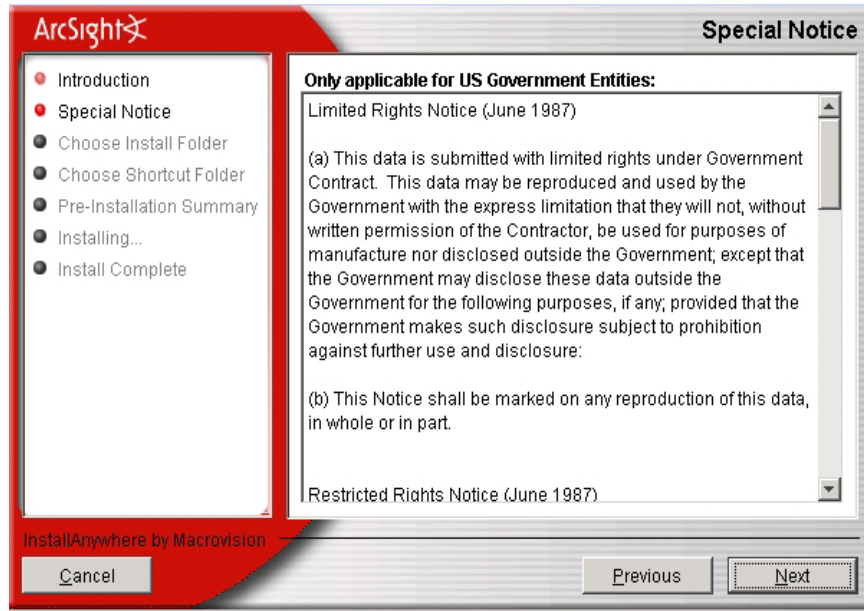
Platform	Installation File
Linux	ArcSight-4.5.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-4.5.x.nnnn.y-Console-Win.exe
Solaris	ArcSight-4.5.x.nnnn.y-Console-Solaris.bin
Macintosh	ArcSight-4.5.x.nnnn.y-Console-MacOSX.bin



Read the introductory text in this panel and click **Next**.



Read the text in the following panel and click **Next** when you are done.

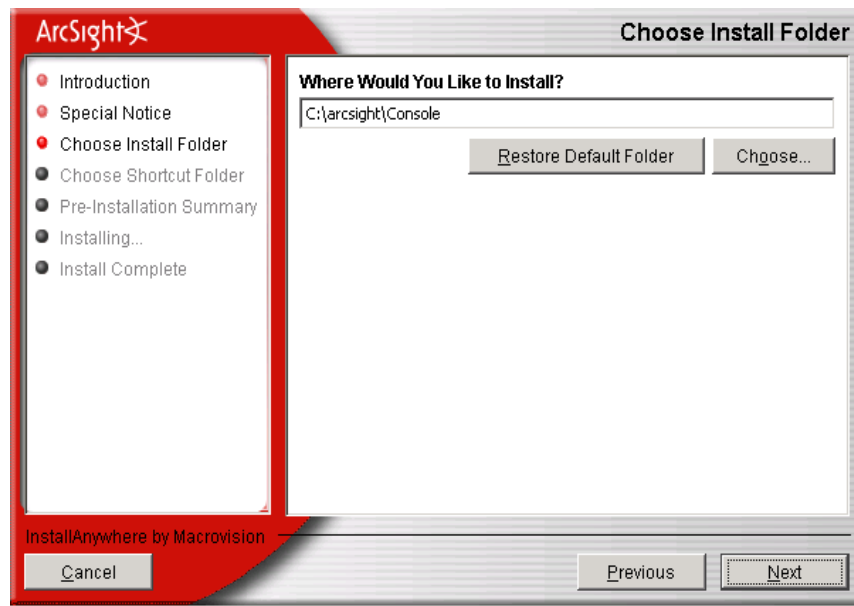


Navigate to an existing folder where you want to install the Console or accept the default and click **Next**. If you specify a folder that does not exist, the folder gets created for you.

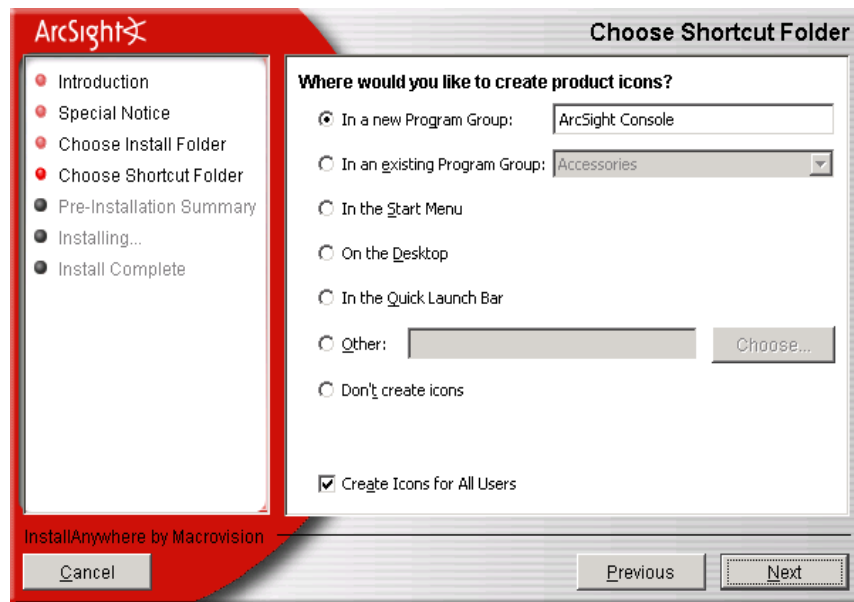


Caution

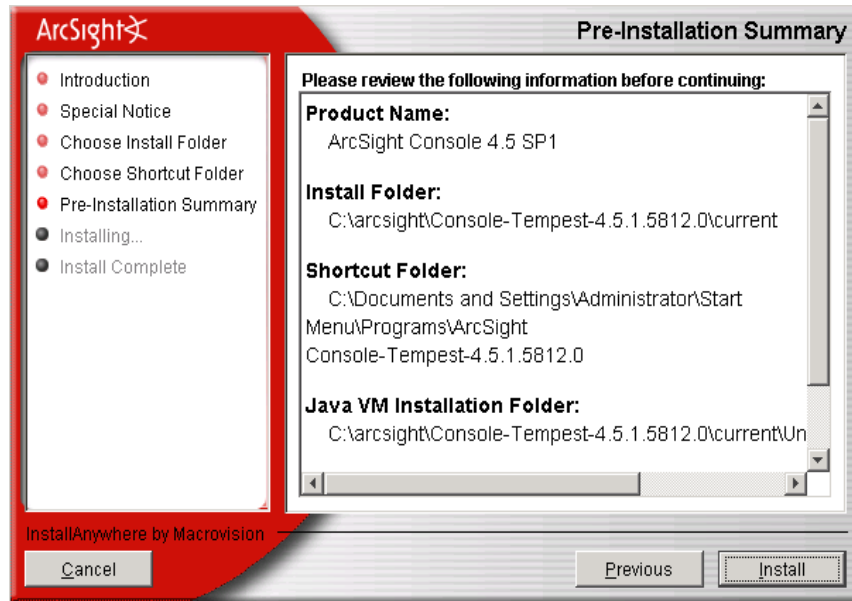
On Windows Vista (64-bit): Make sure that you have administrative privileges to the C:\, C:\Program Files, and C:\Windows directories because these are protected folders and you will not be able to create files (creating a folder is allowed, but you need administrative privileges to create a file) under them without having administrative privileges. When you try to export a package to one of these protected folders, the Console checks the permissions for the parent folder, and when it tries to write the file, an exception is thrown if the parent folder does not have explicit write permission. As a result, the Console will not be able to export a resource package directly under these folders.



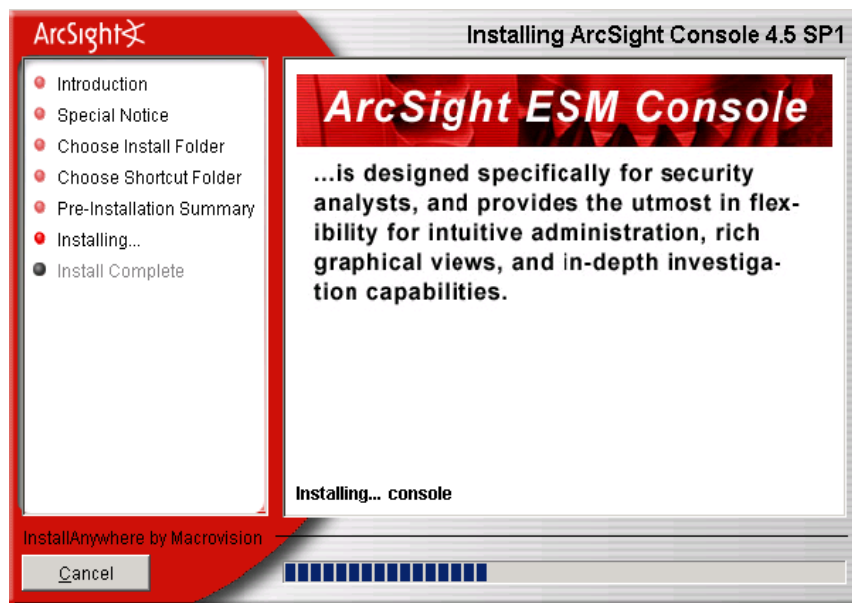
Select where you would like to create a shortcut for the Console and click **Next**.



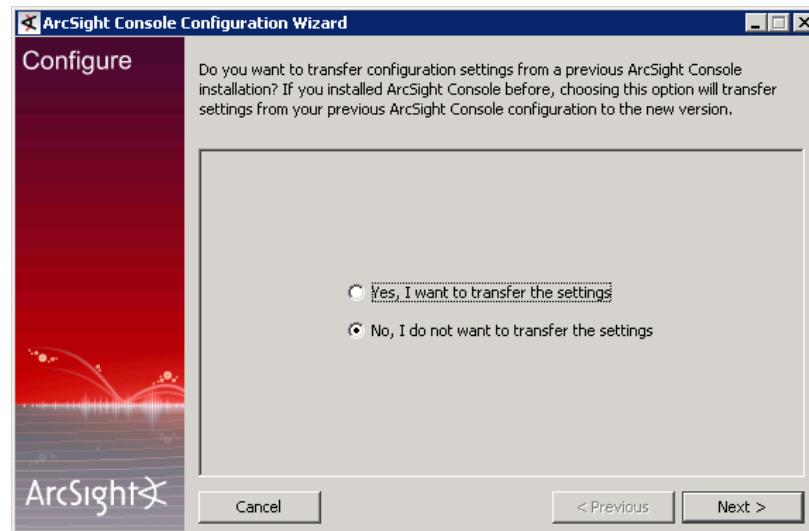
View the summary in the Pre-Installation Summary screen and click **Install** if you are satisfied with the paths listed. If you want to make any changes, use the Previous button to do so.



You can view the installation progress in the progress bar.

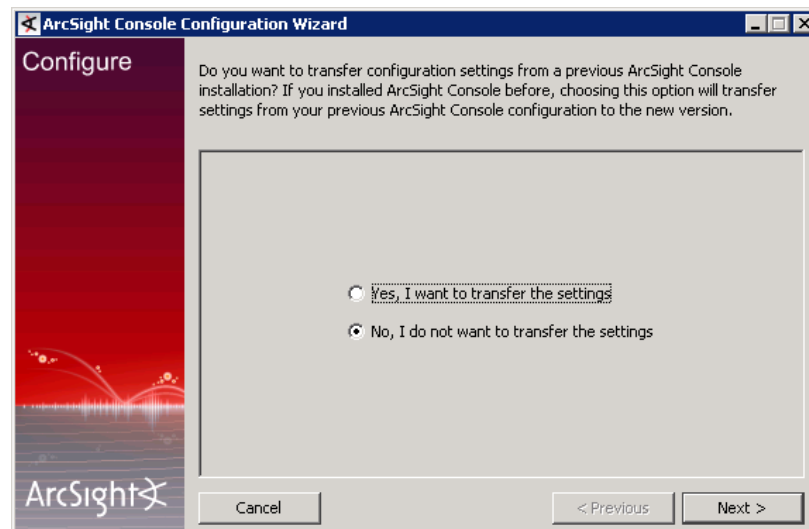


After the Console has been installed, you will see the first configuration screen as shown below:



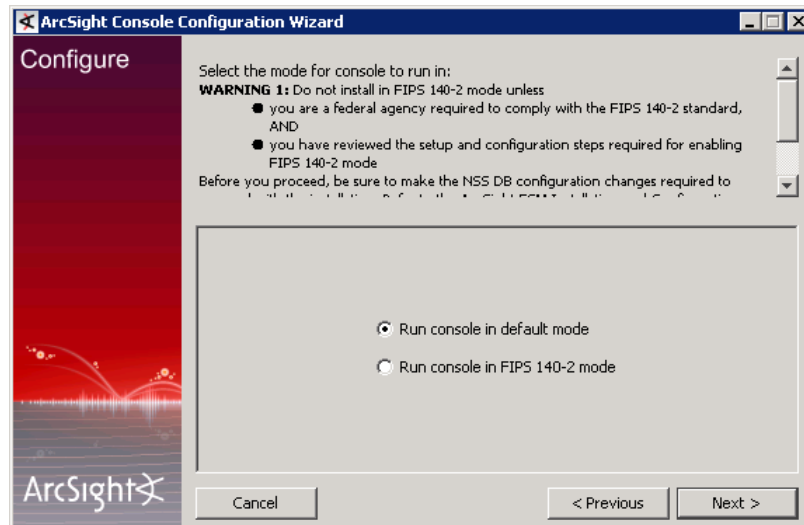
Transferring Configuration from an Existing Installation

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

Next, you will see the following screen:



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

Manager Connection

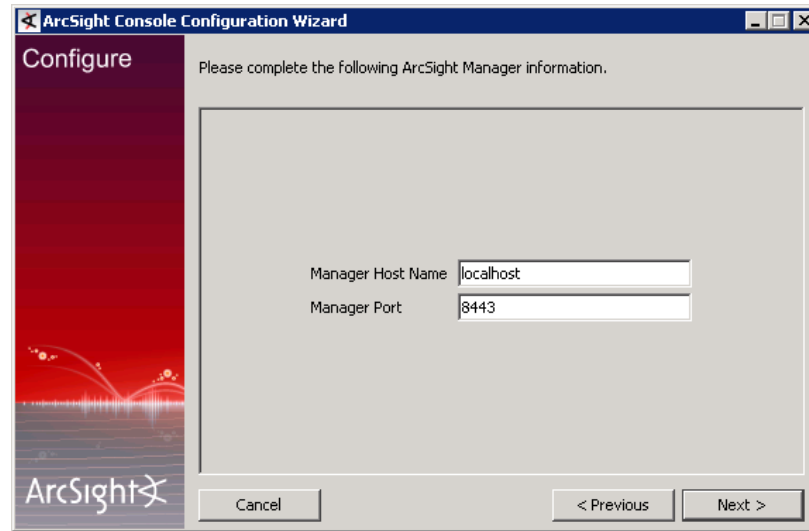
The ArcSight Console Configuration Wizard prompts you to specify the ArcSight Manager with which to connect.

Set the host name on which the Console will communicate with the ArcSight Manager.



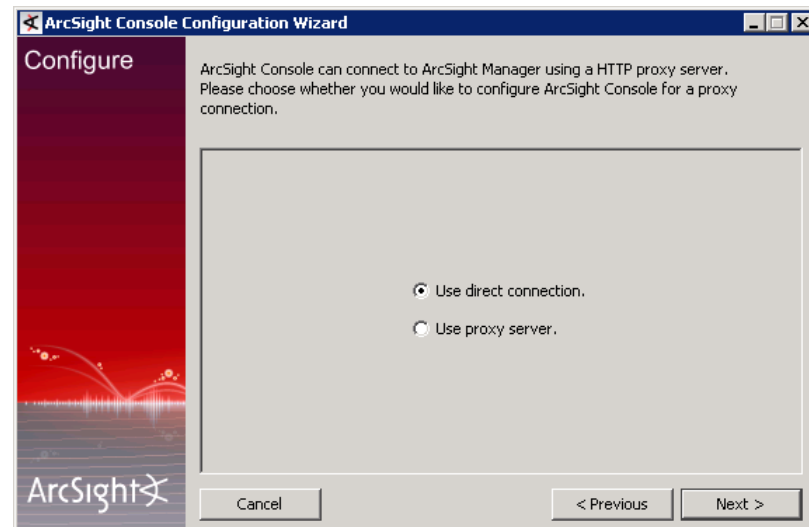
Do not change the Manager's port number.

The Manager hostname must be the same as the Common Name (CN) you used when you created the Manager key pair. Click **Next**.



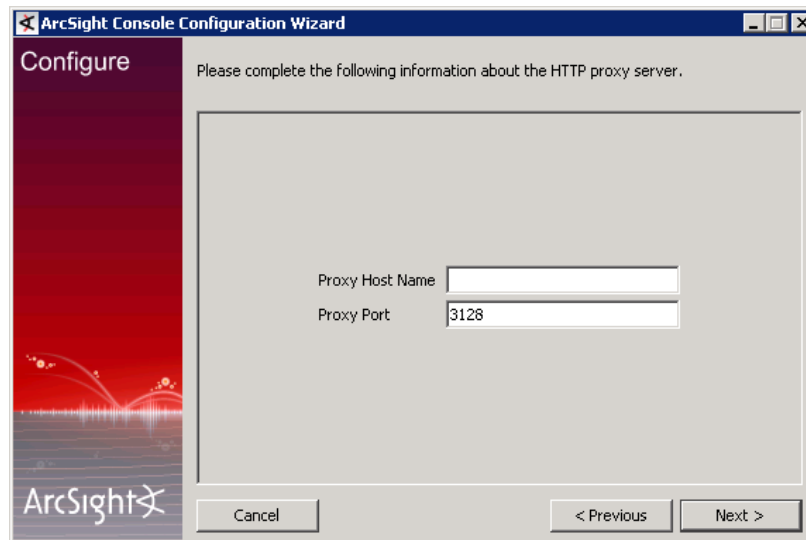
The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'Please complete the following ArcSight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

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



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

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

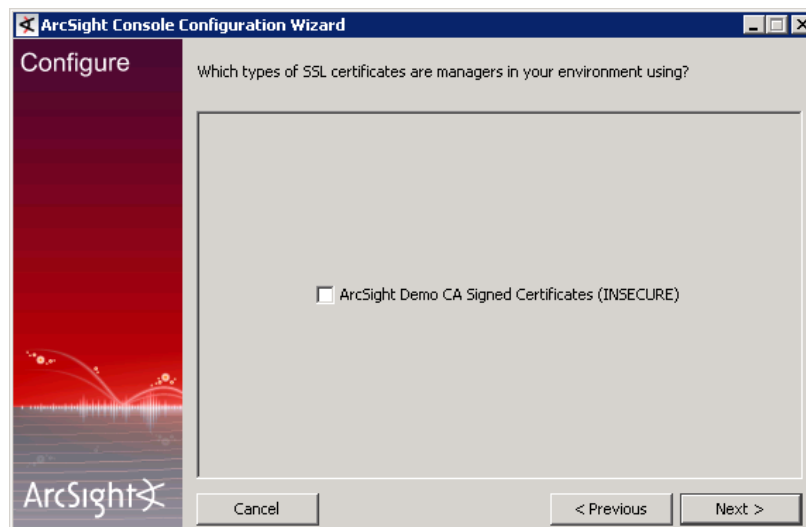


The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background and contains the text 'Please complete the following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

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

SSL Certificate used by Manager

You will see the following screen:



The screenshot shows the 'Configure' step of the ArcSight Console Configuration Wizard. The window title is 'ArcSight Console Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background and contains the text 'Which types of SSL certificates are managers in your environment using?'. Below this text is a single checkbox labeled 'ArcSight Demo CA Signed Certificates (INSECURE)'. At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

Check the checkbox if the Manager you plan to connect to is configured to use a Demo certificate, and click **Next**.

Authentication



In order to use PKCS#11 authentication, you must select one of the SSL based authentication methods.

Caution

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

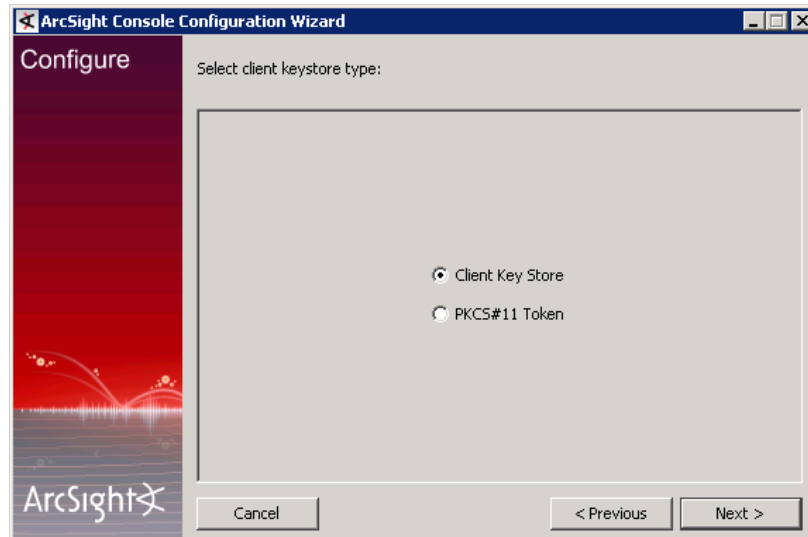


Password Based and SSL Client Based Authentication option currently supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method within the **Password Based and SSL Client Based Authentication** option is not currently supported.

If you select **Password Based Authentication**, you will have to login with a username and password.

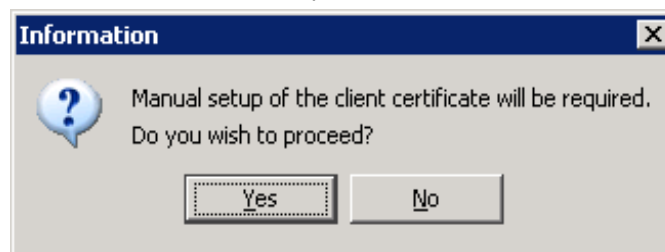
If you select **Password Based and SSL Client Based Authentication**, you will be required to enter both username/password combination and you will be required to setup your client certificate manually. Follow the procedure described in ArcSight ESM *version 4.5 Administrator's Guide* to set up the client certificate.

If you selected **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication**, you will be required to select your SSL client based authentication method.



If you plan to use a PKCS #11 token, you should have the token's software and hardware already set up. If you have not set up the token yet, you can select Client Key Store and continue with the installation. After you have finished installing the Console, you can refer to [Appendix H, Using the PKCS#11 Token, on page 217](#) for instructions on how to set up the token.

If you select **Client Key Store**, you will see a message reminding you to set up the client certificate after the installation completes.

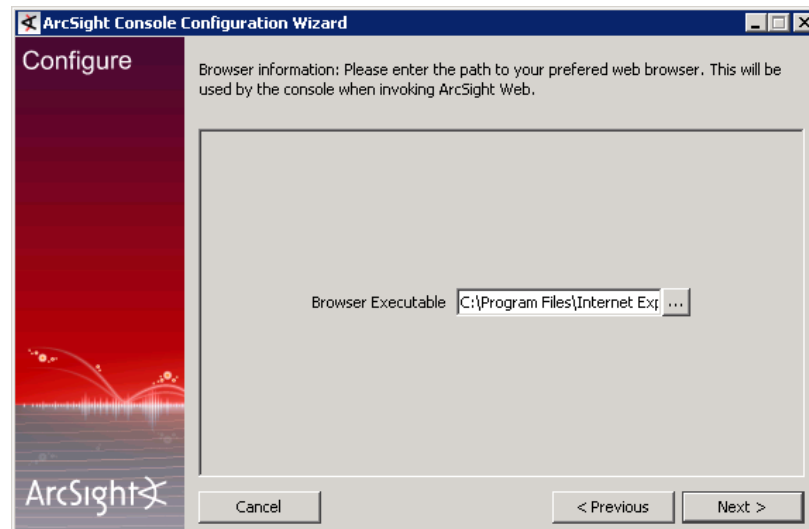


After completing the Configuration Wizard, follow the procedure described in ArcSight ESM *version 4.5 Administrator's Guide* to set up the client certificate.

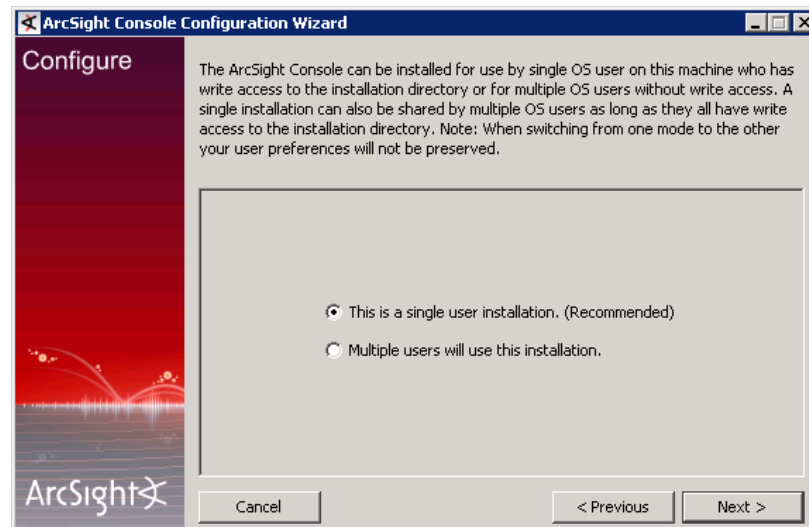
Web Browser

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

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



User Logs and Preferences



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

You can choose from these options:

- This is a single system user installation
 - Select this option when:
 - ◆ There is only one system account on this machine that one or more Console users will use to connect to the Console. For example, a system account, admin, is used by Console users Joe, Jack, Jill, and Jane.

OR

- ◆ All Console users who will use this machine to connect to the Console have their own user accounts on this machine AND these users have write permission to the ArcSight Console's `\current` directory.

Advantage: Logs for all Console users are written to one, central location in ArcSight Console's `\current\logs` directory. The user preferences files (denoted by `username.ast`) for all Console users are located centrally in ArcSight Console's `\current`.

Disadvantage: You cannot use this option if your security policy does not allow all Console users to share a single system user account or all users to write to the ArcSight Console's `\current` directory.

■ Multiple system users will use this installation

Select this option when:

- ◆ All Console users who will be using this machine to connect to the Console have their own user accounts on this machine

AND

- ◆ These users do not have write permission to the ArcSight Console's `\current\logs` directory.

By selecting this option, each user's log and preferences files are written to the user's local directory (for example, `Document and Settings\username\.arcsight\console` on Windows) on this machine.

Advantage: You do not have to enable write permission for all Console users to the Console's `\current` directory.

Disadvantages: Logs are distributed. Therefore, to view logs for a specific time period, you will have to access them from the local directory of the user who was connected at that time.

If you do not enable write permission for all the Console users to the Console's `\current` directory, they can only run the following commands (found in the Console's `\bin\scripts`) from the Console command-line interface:

- ◆ `sendlogs`
- ◆ `console`
- ◆ `exceptions`
- ◆ `portinfo`
- ◆ `websearch`

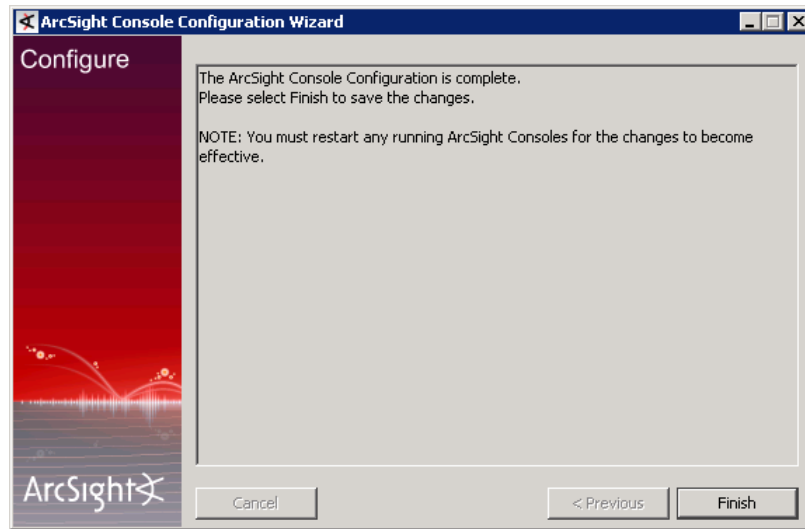
All other commands require write permission to the Console's `\current` directory.



Note

The location from which the Console accesses user preference files and writes logs to depends on the option you select above. Therefore, if you switch between these options after the initial configuration, any customized user preferences may appear to be lost. For example, your Console is currently configured with the "This is a single system user installation" option on a Windows machine. Console user Joe's customized preferences file is located in `<ARCSIGHT_HOME>\Console\current`. Now, you run the `consolesetup` command and change the setting to Multiple system users will use this installation. Next time Joe connects to the Console, the Console will access Joe's preference file from `Document and Settings\joe\.arcsight\console`, which will contain the default preferences.

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



Click **Done** in the next screen.

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

Starting the ArcSight Console



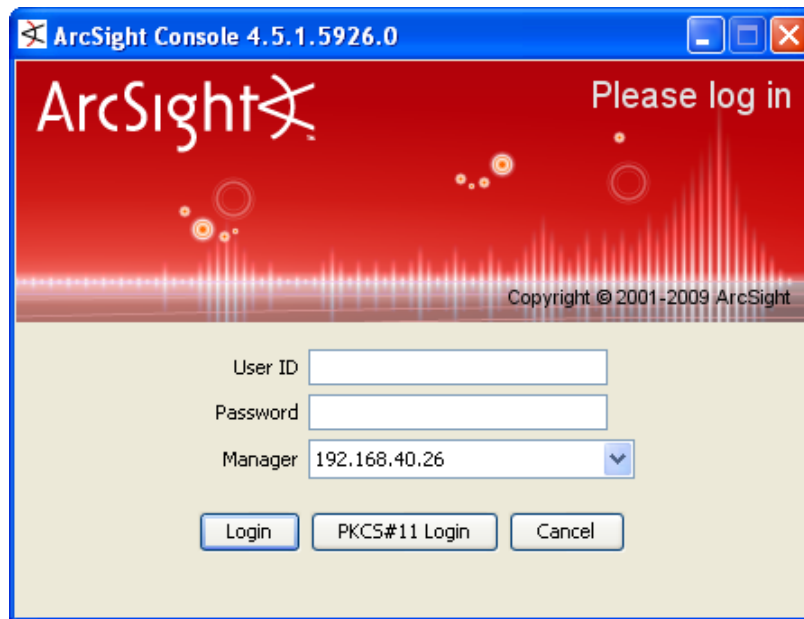
Note

The Manager 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
```

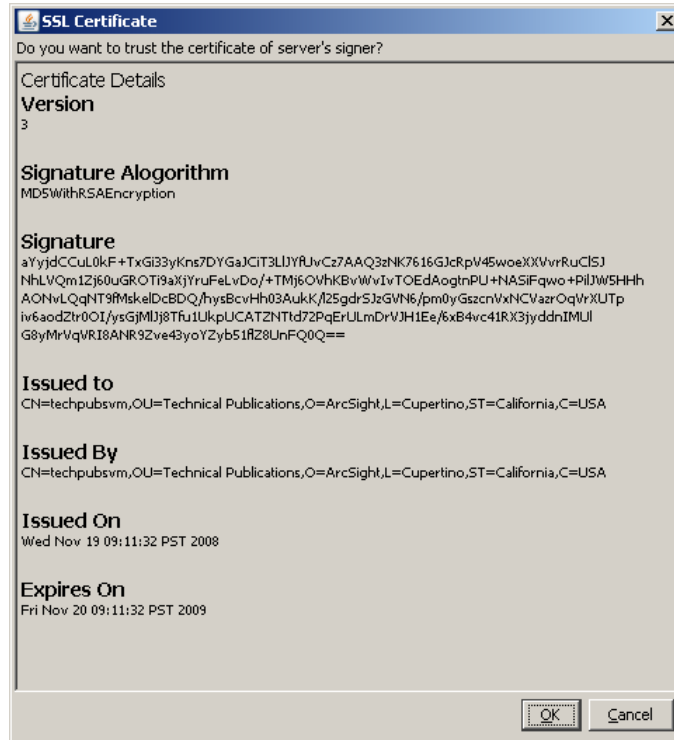
Depending on the client authentication method you selected when installing the Console, you will see the following buttons on the login screen shown above:

If you selected...	You will see the following buttons...
Password Based Authentication	Login Cancel
Password Based and SSL Client Based Authentication	Login Cancel
Password Based or SSL Client Based Authentication	If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: none"> Login (username and password) SSL Client Login Cancel If you selected PKCS#11 Token, you will see <ul style="list-style-type: none"> PKCS#11 Login Login Cancel
SSL Client Only Authentication	If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: none"> Login (username and password) Cancel If you selected PKCS#11 Token, you will see <ul style="list-style-type: none"> PKCS#11 Login (SSL client authentication) Cancel

Logging into the Console

To start the Console, click **Login**

When you start the Console for the first time, after you click Login, if your Manager uses a self-signed certificate, you will get a dialog asking you whether you want to trust the Manager's certificate. 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 following prompt 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.

Uninstalling the ArcSight Console

Before uninstalling the ArcSight Console, exit the current session.

To uninstall on Windows, open the **Start** menu. Run the Uninstall ArcSight Console 4.5 program found under **All Programs->ArcSight Console**. 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
```



Note

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 5

Installing ArcSight Web

This chapter describes the installation and configuration of the ArcSight Web in default mode. To install the Web in FIPS mode, see [Appendix G, Installing ArcSight ESM in FIPS Mode, on page 175](#).



Install ArcSight Web only after you have installed the ArcSight Manager and have it up and running.

The following topics are covered in this chapter:

[“ArcSight Web Supported Platforms” on page 129](#)

[“Using a PKCS#11 Token” on page 130](#)

[“Installing ArcSight Web” on page 131](#)

[“Starting ArcSight Web Manually” on page 140](#)

[“Connecting to ArcSight Web” on page 141](#)

[“Styling ArcSight Web” on page 141](#)

[“Uninstalling ArcSight Web” on page 141](#)

ArcSight Web Supported Platforms



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

The following operating system platforms are supported. The sections which follow describe more detailed requirements by platform.



On 64-bit machines a minimum of 4 GB RAM is required.

Platform	Supported Operating System	Typical System Requirements
Linux	RHEL v4 AS update 8 (32 bit and 64-bit) RHEL v5.3 AS update 2 (32 bit and 64-bit) SUSE Linux 10 SP2 Enterprise Server (64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Microsoft Windows	Microsoft Windows Server 2003 R2 SP2 (32-bit and 64-bit) Microsoft Windows Server 2008 (32-bit and 64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Solaris	Sun Solaris 10 (64-bit)	Sparc-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
IBM AIX	AIX 5L 5.3 (5.3.0.70) 64-bit	Power PC multi-CPU system with 2-16 GB RAM, 2 GB disk space

Web Browsers

ArcSight Web requires a suitable web browser and the Macromedia Flash plug-in, version 8.0 or later. No specific Java version is required for browsers to work with ArcSight Web.

The following table lists supported web browsers:

Platform	Supported Browsers
Solaris	Firefox 2.0
Windows	Internet Explorer 6.0, 7.0, Firefox 2.0, 3.0
Linux	Firefox 2.0, 3.0
Macintosh	Safari 2.0, 3.1, Firefox 2.0, 3.0

Using a PKCS#11 Token



Note

For this release, the use of PKCS#11 token is supported on Windows XP platform only.

Starting ESM v4.0 SP2, 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. PKCS#11 is a public key cryptography standard which defines an API to cryptographic tokens.

You can use the PKCS#11 token regardless of the mode that the client is running in - with clients running in FIPS 140-2 mode or with clients running in the default mode. See [Appendix H, Using the PKCS#11 Token, on page 217](#) for details on using a PKCS #11 token with ArcSight Web.

Installing ArcSight Web



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.

ArcSight Web is a web server that acts as an intermediary between the ArcSight Manager and user sessions in web browsers such as Internet Explorer. ArcSight Web can operate outside a firewall that protects the Manager.

To install ArcSight Web, run the appropriate executable file for your target platform. On Linux and Solaris be sure that you are **not** logged on as root:

Platform	Installation File
Windows	ArcSight-4.5.x.nnnn.y-Web-Win.exe
AIX	ArcSight-4.5.x.nnnn.y-Web-AIX.bin
Linux	ArcSight-4.5.x.nnnn.y-Web-Linux.bin
Solaris	ArcSight-4.5.x.nnnn.y-Web-Solaris.bin

- 1 Read the installation process checklist and click **Next**.
- 2 Read the introduction and click **Next**.
- 3 Read the notice and click **Next**.
- 4 Enter or navigate to the directory where you want to install ArcSight Web.

You can install ArcSight Web on the same host as the ArcSight Manager or on a separate machine that has network access to the Manager. You may run multiple instances of ArcSight Web against the same ArcSight Manager, and each instance can be configured with different styling, if desired.

Click **Next**.

- 5 Choose a location where you would like to create a shortcut for ArcSight Web and click **Next**.

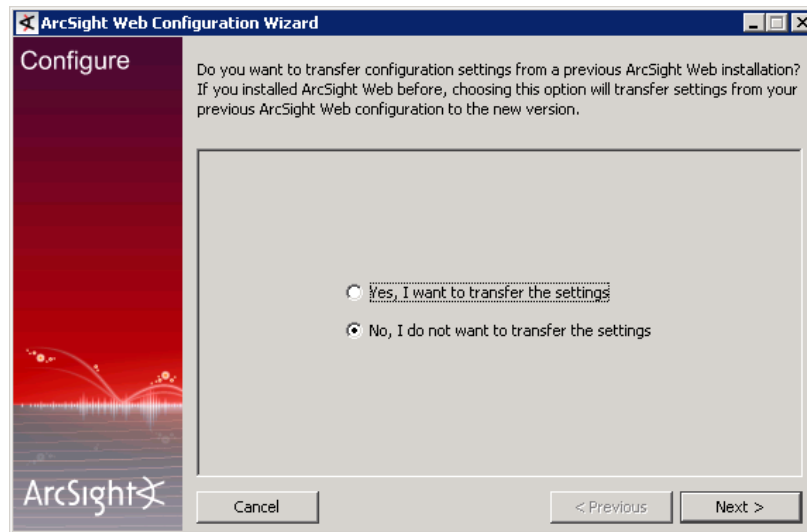
You can monitor the installation progress in the next screen.

The configuration wizard starts up automatically at the end of the installation.



If you are installing in console mode you will have to manually run the setup program by typing `arcsight websetup` in the installed `<ARCSIGHT_HOME>\bin` directory.

The wizard prompts you to pick if you would like to transfer configuration options from a previous installation of ArcSight Web.



Select **No, I do not want to transfer the settings** and click **Next**.

Setting up SSL Client Authentication

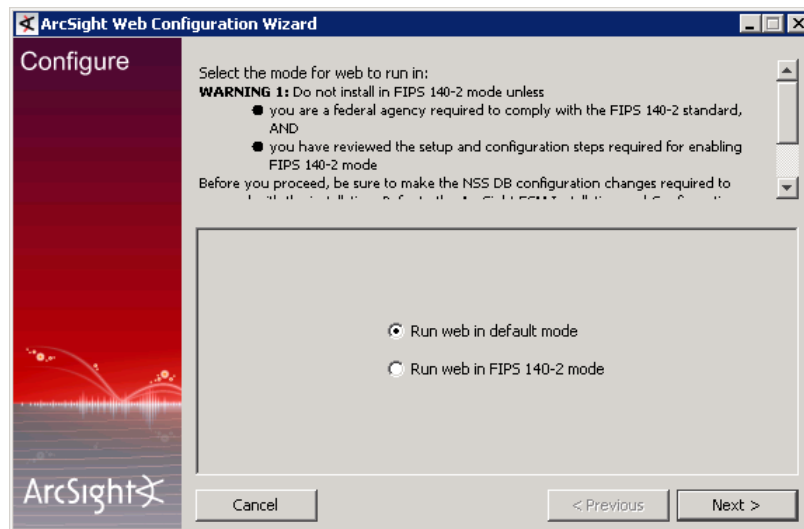
If you would like to set up SSL client authentication, you will need to replace the `cacerts` file in your ArcSight Web's `<ARCSIGHT_HOME>\jre\lib\security` with the `cacerts` file from your Manager's `<ARCSIGHT_HOME>\jre\lib\security` folder **before** you configure ArcSight Web. Follow the steps in "Setting up SSL Client Authentication for ArcSight Web" section in Chapter 4 in the ArcSight ESM *version 4.5 Administrator's Guide*.

Selecting the Mode in which to Configure ArcSight Web

You will be prompted to select the mode in which to configure ArcSight Web:



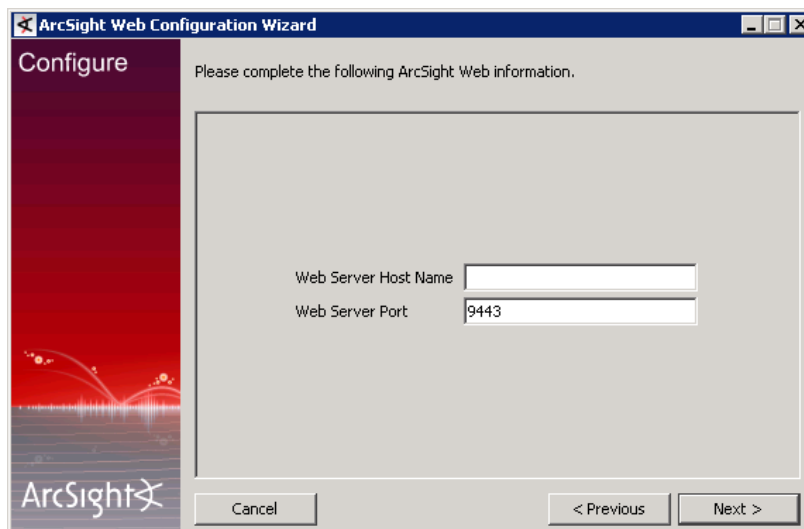
Keep in mind that once you have made your choice and clicked Next, you can not revert to this screen.



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

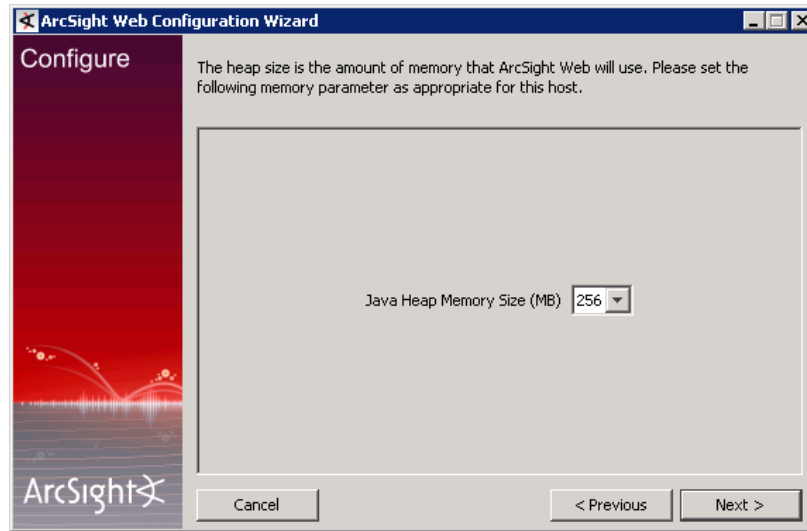
Web server Host Name and Port

Enter the web server's host name and port. The default is localhost and port 9443. To avoid restricting the server to local testing only, enter a name for the server, such as the machine's host name.



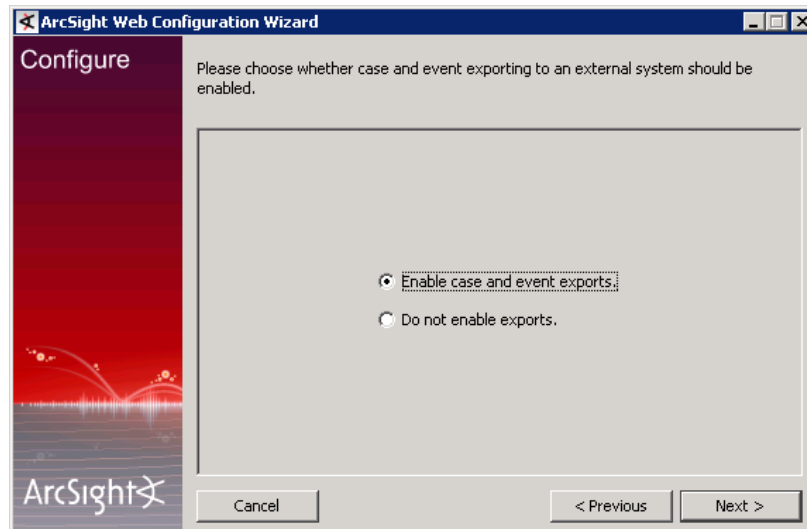
Java Heap Memory Size

Select the heap memory size. The default is 256 MB.



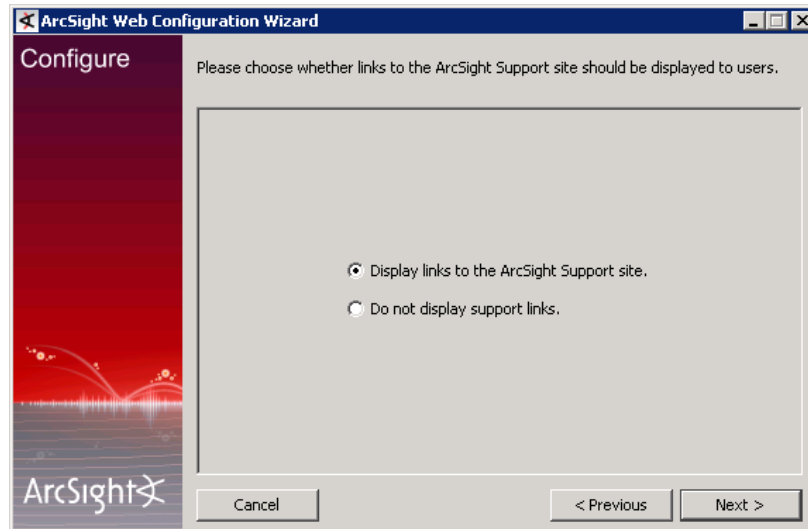
Enable Case and Events Exports

If you want to export cases and events, select **Enable case and event exports**.



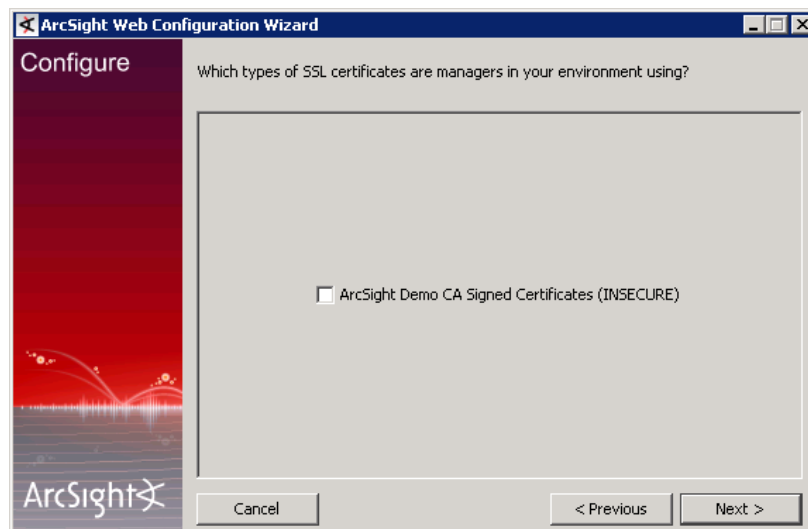
Display Links to Support Web site

Choose whether to display a link to ArcSight Customer Support on the home page.



Is the Manager Configured to use Demo Certificate?

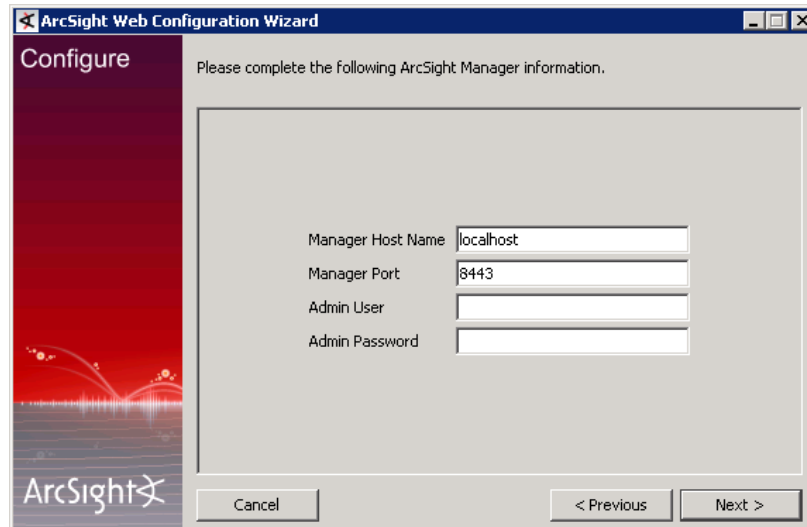
You will be prompted to select if the ArcSight Manager has been configured to use a Demo certificate, if you opted to configure ArcSight Web in default mode.



If your Manager is configured to use a self-signed or CA Signed certificate, leave this panel unchecked, finish this Web setup wizard, then use the keytoolgui to import your Manager certificate manually. See the section, "Understanding SSL Authentication" in the *ArcSight ESM Administrator's Guide, v4.5*.

ArcSight Manager Host Name and Port

Make sure that the Manager is up and running. Then, enter the ArcSight Manager's host name, port, admin user and admin password.

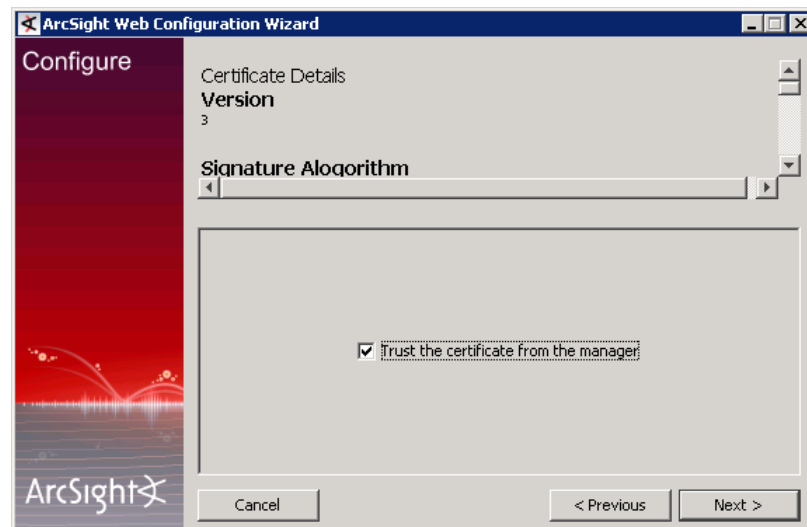


The screenshot shows the 'Configure' step of the ArcSight Web Configuration Wizard. The window title is 'ArcSight Web Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background with the text 'Please complete the following ArcSight Manager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

If you opted to configure ArcSight Web in FIPS 140-2 mode, go to ["Authentication" on page 138](#).

Trust Manager Certificate

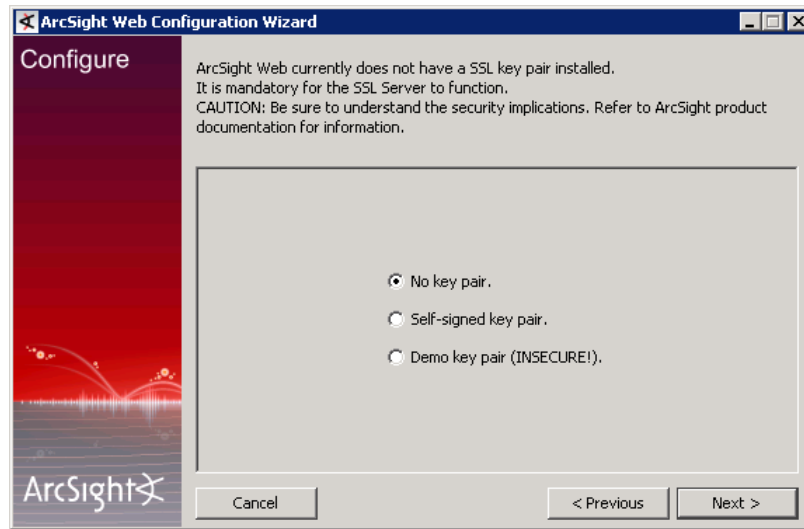
If the Manager uses a self-signed certificate, you will see the following dialog asking you whether you trust the Manager's certificate. Check the checkbox and click **Next**



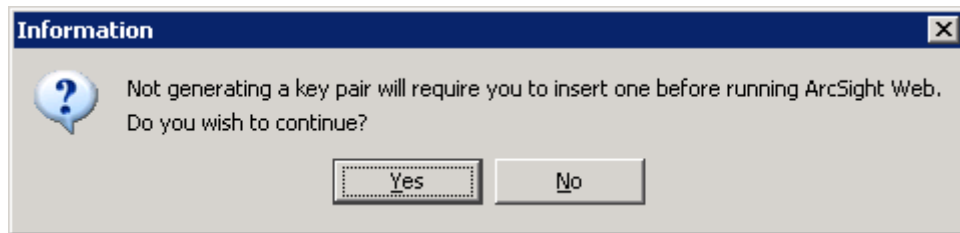
The screenshot shows the 'Certificate Details' step of the ArcSight Web Configuration Wizard. The window title is 'ArcSight Web Configuration Wizard'. The left sidebar is the same as the previous step. The main area has a light gray background with the text 'Certificate Details'. Below this text are two sections: 'Version' with the value '3' and 'Signature Algorithm' with a dropdown menu. At the bottom is a checkbox labeled 'Trust the certificate from the manager' which is checked. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

Select Type of Key Pair

You will be prompted to select the type of key pair you want to use:



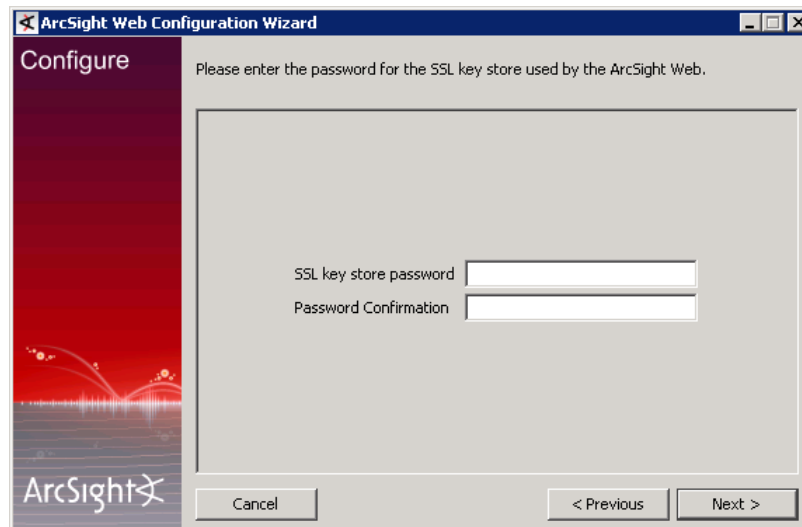
If you select **No key pair**, you will see the following warning:



If you select **Self-signed key pair**, you will be prompted to enter the details of the SSL certificate to be issued:



You will also be asked to set up a keystore password.



The screenshot shows the 'Configure' step of the ArcSight Web Configuration Wizard. The window title is 'ArcSight Web Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background. At the top, it says 'Please enter the password for the SSL key store used by the ArcSight Web.' Below this, there are two text input fields: 'SSL key store password' and 'Password Confirmation'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

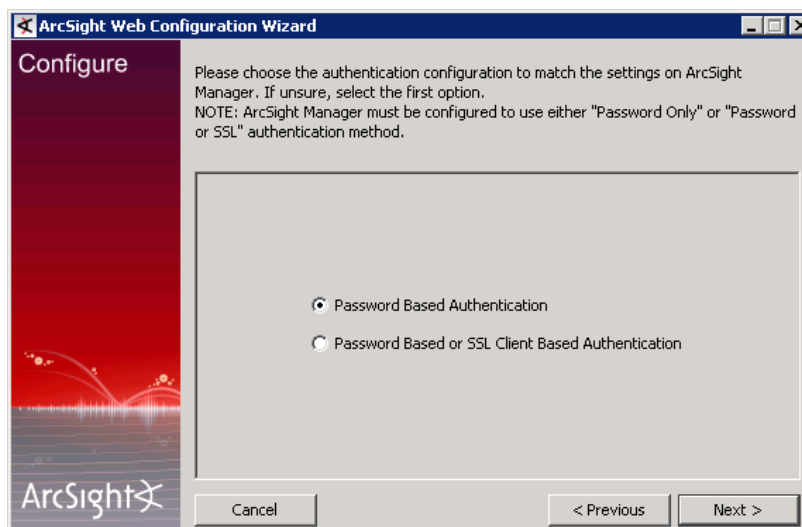
If you selected the **Demo key pair** option, you will also see the screen above that prompts you for a password for the SSL Key store used by ArcSight Web.

Authentication

Choose the type of client authentication you want to use.



If you plan to use a PKCS #11 token with ArcSight Web, be sure to select **Password Based or SSL Client Based Authentication** and make sure that your Manager is configured to use the same authentication method.

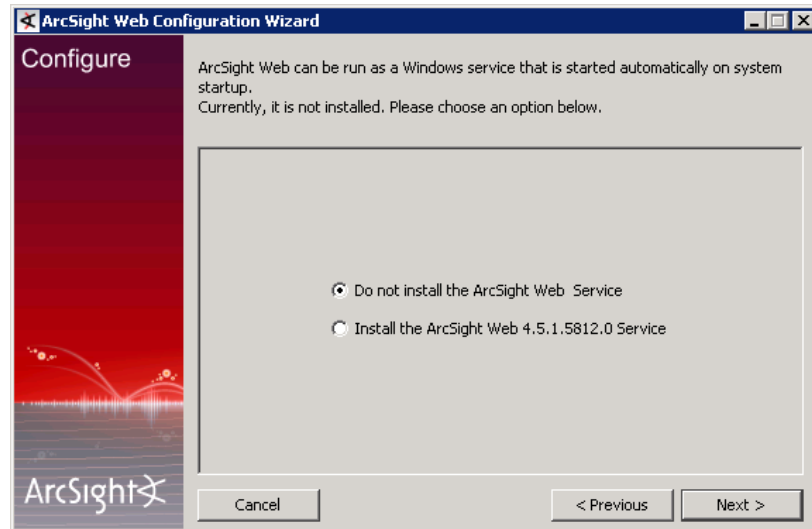


The screenshot shows the 'Configure' step of the ArcSight Web Configuration Wizard. The window title is 'ArcSight Web Configuration Wizard'. The left sidebar has a red background with the ArcSight logo. The main area has a light gray background. At the top, it says 'Please choose the authentication configuration to match the settings on ArcSight Manager. If unsure, select the first option.' Below this, there is a note: 'NOTE: ArcSight Manager must be configured to use either "Password Only" or "Password or SSL" authentication method.' Below the note, there are two radio button options: 'Password Based Authentication' (which is selected) and 'Password Based or SSL Client Based Authentication'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

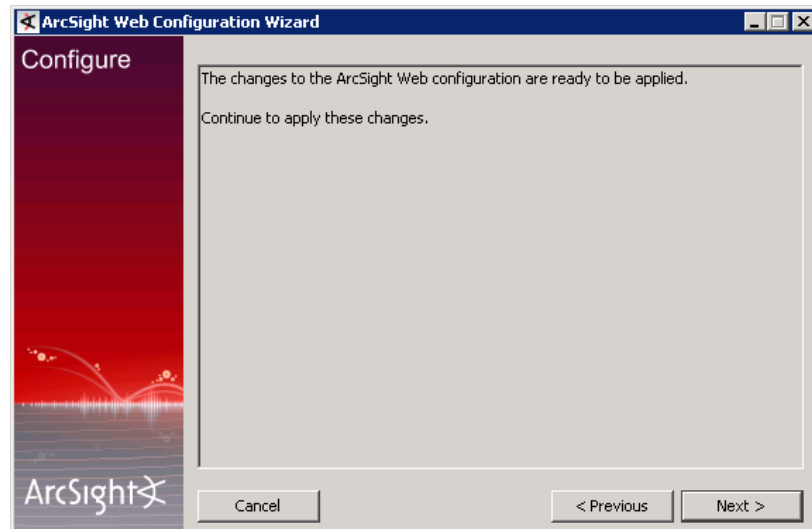
Click **Next**.

Setting ArcSight Web as a Service or Daemon

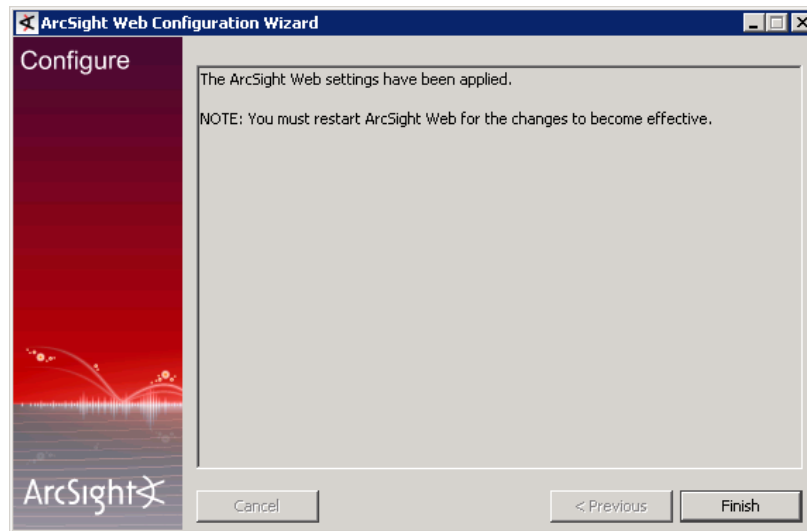
Choose whether ArcSight Web should be installed as service or not.



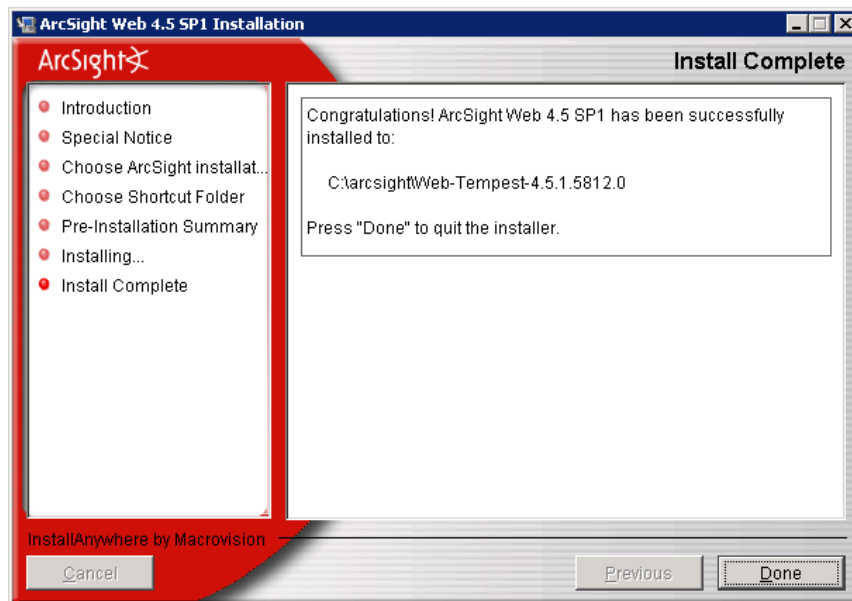
You will see the following screen:



Click **Next** and you will see the following screen:



Click **Finish** to save changes. You will see the following screen which gives you the location where ArcSight Web has been installed.



Click **Done**.

Starting ArcSight Web Manually

To start ArcSight Web manually, go to the Web's `<ARCSIGHT_HOME>\bin` directory and execute the command:

```
arcsight webserver
```


Connecting to ArcSight Web

Go to the URL <https://<hostname>:9443/arc sight/app> in a browser, where hostname is the name configured in websetup. ArcSight Web presents an interface that is similar to that of the ArcSight Console, allowing authenticated users to view dashboards, data monitors and other resources.

Styling ArcSight Web

To change logo images and colors, create the file `config\web\styles.properties` by copying either `example.styles.properties` or `full.styles.properties`. Inside either file you will find information about those properties that can be changed, along with example values. After making changes to the properties file, restart the web server to see the effect of those changes.

Branding and style changes are visible to anyone using that instance of ArcSight Web.

Uninstalling ArcSight Web

Stop ArcSight Web server before uninstalling it.

To uninstall on Windows, open the **Start** menu. Run the Uninstall ArcSight Web 4.5 program found under All Programs | ArcSight Web. If a shortcut to the Web was not installed on the Start menu, locate the `<ARCSIGHT_HOME>\UninstallerData` folder and double-click:

`Uninstall_ArcSight_Web.exe`

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

`./Uninstall_ArcSight_Web`



- The UninstallerData directory contains a file `.com.zerog.registry.xml` with Read, Write, and Execute permissions for everyone. You can change the permissions to Read and Write for everyone (that is, 666).
- The Uninstaller does not remove all the files and directories under the ArcSight Web home folder. Please delete these folders manually after the uninstallation is complete.

Installing ArcSight SmartConnectors

The ArcSight system monitors security events throughout the enterprise using a phalanx of distributed SmartConnectors. This chapter covers the following topics:

[“Deployment Considerations” on page 143](#)

[“Installing ArcSight SmartConnectors” on page 143](#)

After you have installed the ArcSight Manager, you should install ArcSight SmartConnectors for all of the devices that you want ArcSight to monitor. The term device can refer to a firewall, or a software component such as an intrusion prevention system or a host syslog. A device is a source of security events. Some ArcSight SmartConnectors require you to configure the device before you can receive events.

For more information on how to install a particular ArcSight SmartConnector and configure the device, refer to the ArcSight SmartConnector *User's Guide* for basic SmartConnector installer instructions and also refer to the vendor-specific ArcSight SmartConnector *Configuration Guide* for the device you are using.

Deployment Considerations

This section explains the things you will have to keep in mind before deploying the ArcSight SmartConnectors.

ArcSight provides dozens of SmartConnectors custom designed to monitor security events from Intrusion Detection Systems (IDSs), firewalls, network management devices, operating system security components and other sources of security events.

In addition to vendor-specific SmartConnectors available from ArcSight, the ArcSight FlexConnector allows you to create SmartConnectors that are tailored to your situation and specific security event data. FlexConnector types include file reader, regular expression file reader, time-based database reader, syslog, and Simple Network Management Protocol (SNMP) readers.

Installing ArcSight SmartConnectors

Before installing SmartConnectors, confirm that the ArcSight Manager and Database components are up and running. Log in as the 'arcsight' user (or an existing user with sufficient admin privileges). Install ArcSight SmartConnectors using the SmartConnector

Installation Wizard appropriate for the target platform. In the wizard, you specify the particular SmartConnector to be installed.



At a minimum, SmartConnectors should be running version 4021 to communicate with an ESM version 4.5 Manager.

For an overview of the SmartConnector installation and configuration process, see the *SmartConnector User's Guide*. For complete installation instructions for a particular SmartConnector, see the configuration guide for that connector. The product-specific configuration guide provides specific device configuration information, installation parameters, and device event mappings to ArcSight ESM fields. For instructions on installing the SmartConnectors in FIPS mode see *Installing FIPS Compliant SmartConnectors* technical note.

Establishing Initial ArcSight Resources

This chapter describes the initialization of resources in a new ArcSight installation. Resources include users, rules, assets (the components of your network), and other installation-specific items. This chapter covers the following topics:

[“Defining Zones and Assets” on page 145](#)

[“Defining Asset Categories” on page 148](#)

[“Creating Customers and Users” on page 149](#)

[“Tuning Data Monitors and Rules” on page 150](#)

To complete your ArcSight deployment, describe your assets and network characteristics to customize the installation for your enterprise. The following instructions will explain how to create and configure:

- Zones, Locations, and Networks
- Assets and Asset Ranges
- Asset Categories
- Customers

For more information about initializing the ArcSight System, refer to ArcSight ESM v4.5 *Administrator's Guide*.

Defining Zones and Assets

Use the following procedure to document your IP address ranges:

- 1 Begin by creating Zones. Zones group Connectors logically into functional areas (Sales, Operations, etc.), geographical regions (Denver, Pittsburgh, etc.), or some other meaningful organization. Zones can overlap; that is, a SmartConnector can be assigned to more than one zone. Zones are particularly useful when IP addresses are reused within a network (for example, with DHCP).

Login to the ArcSight Console. In the Navigator window, choose **Assets** from the menu and click the **Zones** tab. Right-click in an appropriate group and select **New Zone**. Enter a name for the new Zone. Repeat until all Zones have been defined.

The screenshot shows the 'Inspect/Edit' dialog box with the 'Zone Editor' tab selected. The 'Zone' section contains the following fields:

Name	
Start Address	0.0.0.0
End Address	0.0.0.0
Dynamic Addressing	<input type="checkbox"/>
Location	Select a Location
Network	Select a Network

The 'Common' section contains the following fields:

External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

The 'Assign' section contains the following fields:

Owner	
Notification Groups	

At the bottom of the dialog, there is a 'Name' field with the text 'Enter a name for this resource' and buttons for OK, Cancel, Apply, and Help.

- 2 Create Locations the same way. In the Navigator pane, choose **Assets** from the menu. Click the **Locations** tab. Right-click in an appropriate group and select **New Location**.
- 3 Next, define your Assets. In the Navigator pane, choose **Assets** from the menu. Click the **Assets** tab.
- 4 For each range of IP addresses to be protected, right-click the appropriate Asset Group and select **New Asset Range**.

- 5 In the Asset Range Editor, enter a **Name**, **Start Address**, **End Address**, **Location**, and **Zone** for the new Asset Range.

Asset Range	
Name	
Start Address	0.0.0.0
End Address	0.0.0.0
Location	Select a Location
Zone	Select a Zone

Common	
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

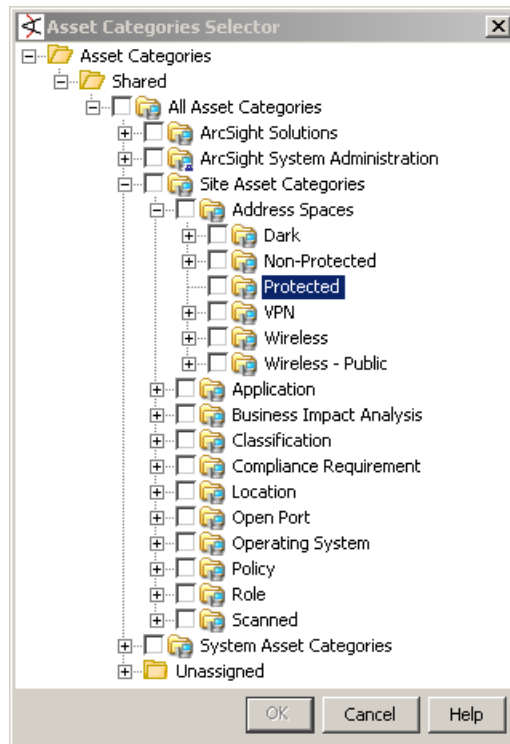
Assign	
Owner	
Notification Groups	

(Name)
(Description)

OK Cancel Apply Help

- 6 Click the **Categories** tab and click the **Add** button to assign the new Asset Range to an Asset Category. Select the **Asset Categories/Shared/All Asset Categories/Site Asset Categories/Address Spaces/Protected** category and click **OK** to dismiss the Asset Categories Selector dialog.

- 7 Review your Asset Categories using the **Categories** tab of the Assets pane in the Navigator panel, as shown below.

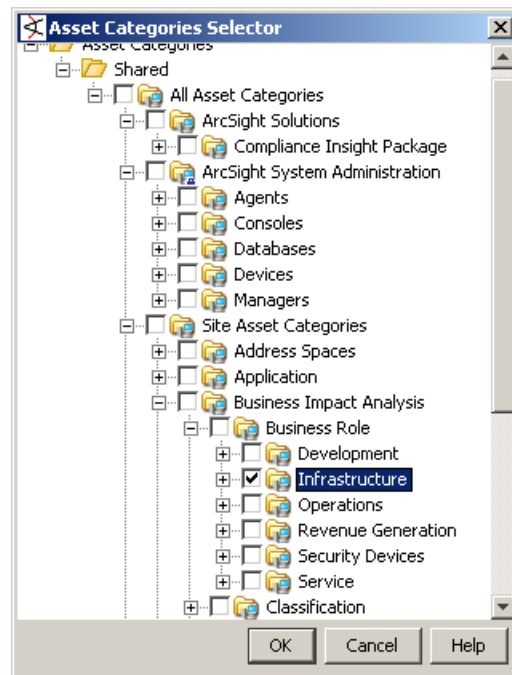


- 8 Update your SmartConnectors to use the Zones you have defined. Examine each SmartConnector in the Navigator pane and select **Configure** from the context menu. On the Networks tab, make sure that the SmartConnector is associated with the appropriate Network resources.

Defining Asset Categories

Follow the steps below to assign Business Impact Analysis and Criticality Asset Categories to your Assets and Asset Ranges:

- 1 Associate your Assets and Asset Ranges with their business function by opening the **Asset** or **Asset Range** in the editor. On the Categories tab, click the **Add** button and choose from the **Business Impact Analysis** categories. One Asset may have several Business Impacts, such as "Secret" and "Operations."



- 2 Associate your Assets with the appropriate Criticality categories (Very High, High, Medium, Low, or Very Low).

Creating Customers and Users

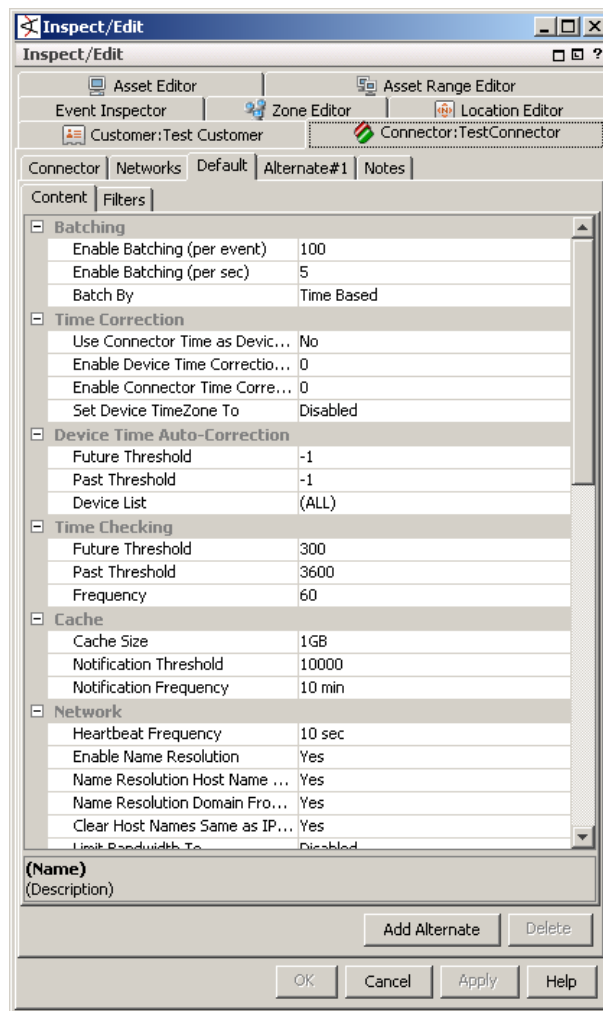
If your ArcSight installation will serve more than one organization, you may want to create Customers and update specific SmartConnectors to refer to particular Customers. Customers are typically used by Managed Security Service Providers (MSSPs).

To associate Customers with specific SmartConnectors:

- 1 Define your Customers. In the Navigator pane.
- 2 Choose **Customers** and select **New Customer** from the context menu.
- 3 Enter Customer information in the Customer Editor and click **OK**.

Associate Customers with Connectors. In the Navigator pane, choose **Connectors**. Right-click a SmartConnector and select **Configure** from the context menu. In the SmartConnector Editor, click the **Default** tab. Specify a Customer URI in the Network section of the Content tab.

The URI field value can be a Velocity template (for example, “/All Customers/\$agentAddress”) or a literal string.



Tuning Data Monitors and Rules

Before putting ArcSight into production, review the built-in Data Monitors and Rules. You may want to disable any Data Monitors or Rules which are not relevant.

To view Data Monitors, choose **Dashboards** from the Navigator window menu and click the **Data Monitors** tab. If you do not need a particular Data Monitor, right-click on it and select **Disable Data Monitor** from the context menu.

To view Rules, choose **Rules** from the Navigator window menu. Right-click a specific Rule and select **Disable Rule** from the context menu.

Appendix A

Configuring an Existing Oracle Installation

This appendix provides tips for implementing ArcSight with an existing or custom Oracle installation. The ArcSight Database Installer detects and adjusts to an existing Oracle installation. Using standard ArcSight tools verifies minimum platform requirements and helps ensure consistency across deployments.

This appendix covers the following topics:

- [“Creating an ArcSight Instance with an existing Oracle Installation” on page 151](#)
- [“Initializing the ArcSight Schema with an Existing ArcSight Instance” on page 152](#)
- [“Installing Oracle DBMS Without Using the ArcSight Database Installer” on page 152](#)

ArcSight recommends that you always use the ArcSight Database Installer to install and configure the Oracle DBMS and create the ArcSight instance. The ArcSight Database Installer ensures that the Oracle installation and the ArcSight instance conform to ArcSight's time-tested configuration for optimal performance, reliability, and security. For example, the ArcSight Database Installer includes only necessary Oracle components and includes workarounds for known Oracle security vulnerabilities.

Creating an ArcSight Instance with an existing Oracle Installation

If Oracle is already installed and you must use the existing installation for some reason, perform the following steps to create the ArcSight instance and initialize the ArcSight Database.

- 1 Log in as root on the database machine.
- 2 Run the ArcSight Database Installer wizard.
- 3 Choose **Install ArcSight Software Only.**



ArcSight recommends that you always install ArcSight Database software in a standard location, such as `/usr/local/arc sight/db` on Unix, or `c:\arc sight\db` on Windows.

- 4 Continue to the end of the Database Installer wizard.
- 5 Open a command window to the directory where the ArcSight Database software is installed (`<ARCSIGHT_HOME>`) and run the following command:

```
bin\arcsight database create
```

6 Choose **Create and configure the ArcSight instance only**



Note

If you require a special template, edit or replace the file `installer/oracle10g/unix/dbca/ArcSight_Large.dbt` and select the **Large** template from the drop-down menu. (If your database machine has a 64-bit operating system, 8 CPUs, and 16 GB of memory, for example, you can overwrite `ArcSight_Large.dbt` with `ArcSight_64bit_8CPU_16GB.dbt`.)



Caution

Before proceeding, choose the appropriate template for your needs. Refer to [“Selecting an ArcSight Database Template” on page 30](#), for more information.

Initializing the ArcSight Schema with an Existing ArcSight Instance

If the ArcSight instance already exists, perform the following steps to initialize (or reinitialize) the ArcSight schema:

- 1 Log in as root on the database machine.
- 2 Run the ArcSight Database Installer wizard.
- 3 Choose **Install ArcSight Software Only**.
- 4 Continue to the end of the Database Installer wizard.
- 5 Open a command window to the directory where the ArcSight Database software is installed (`<ARCSIGHT_HOME>`) and run the following command:


```
bin\arcsight database init
```
- 6 Choose the option (create or recreate) which matches your needs.
- 7 Complete the steps of the wizard.

Installing Oracle DBMS Without Using the ArcSight Database Installer

If you need to install Oracle DBMS without using the ArcSight Database Installer—which is not recommended—ArcSight provides response files that make the process more likely to succeed.

To extract the ArcSight installation files, including the response files, perform the following steps:

- 1 Log in as root on the database machine.
- 2 Run the ArcSight Database Installer wizard.
- 3 Choose **Install ArcSight Software Only**.
- 4 Continue to the end of the Database Installer wizard.
- 5 You will find the response files under the installation directory in:

`installer/oracle10g/unix/response`



If you use an ArcSight response file, only the core Oracle9i DBMS and the Partitioning option will be installed.

Using UNCOMPRESSED Archive Type

When Partition Archiver is set to Archive Type UNCOMPRESSED, it leaves the files in the partition uncompressed, thus enabling you to compress, encrypt, and sign files later with an archiving tool of your choice.



If you have opted for the UNCOMPRESSED archive type, you must reactivate the archived partitions in the same order in which they were created, that is oldest to the newest. For example, if you created partitions 20060101 thru 20060105 in that order and you want to reactivate partitions 20060101 thru 20060103, you must start by reactivating 20060101 first, then 20060102 and lastly 20060103.

The uncompressed files for a partition are placed in a subdirectory, created automatically for that partition, in the Archive Directory. The subdirectories are named using the format `arc_event_PartitionName`, where PartitionName is of the format `yyyymmdd`. For example, for a partition created for April 1, 2006, a subdirectory named `arc_event_20060401` is created in your Archive Directory.

You will find these files in a subdirectory:

- Oracle dump file (`arc_event_data_PartitionName.dmp`)
- Oracle export log file (`arc_event_data_PartitionName.exp.log`)
- Oracle data files (`arc_event_data_PartitionName_nn.dbf`)

There can be multiple data files if the partition has more than 4 GB of data.

ArcSight recommends that you follow these guidelines when using your own tool for archiving:

- Name the resulting archive file using the format `arc_event_PartitionName.ArchiveFileExtension`
Where PartitionName is of the format `yyyymmdd`; for example, partition name for a partition created on April 1, 2006 is 20060401.
ArchiveFileExtension depends on the tool you choose.
- Do not change the file names of any files in the subdirectories created in Archive Directory.

Archiving Uncompressed Files

To archive uncompressed files belonging to a partition, do the following in your archiving tool:

- 1 Select the subdirectory that contains the uncompressed files for archiving

- 2 Set the option that enables the tool to automatically traverse all subfolders (also known as the recursive option) under the specified subdirectory to look for files to add; for example, check the **Subfolders** option in the WinZip wizard.
- 3 Set the option to save the path info for the archived files; for example, Check the **Save** full path info option in the WinZip wizard.

The archive file is placed in the same subdirectory where the uncompressed files are located.

Examples

Example 1: This example lists the steps taken to archive uncompressed files in the partition 20060401. The Archive Directory is `E:\archive`.

- 1 List the data files in the subdirectory for the partition 20060401:

```
E:\archive>dir arc_event_20060401

Directory of E:\archive\arc_event_20060401

05/09/2006  1,728                arc_event_data_20060401.dmp
05/09/2006   560                arc_event_data_20060401.exp.log
05/09/2006 3,823,657,634        arc_event_data_20060401_01.dbf
05/09/2006 3,657,584,358        arc_event_data_20060401_02.dbf
05/09/2006 3,657,584,287        arc_event_data_20060401_03.dbf
```

- 2 Archive the subdirectory for the partition (`arc_event_20060401`) with the command-line version of WinZip with AES256 encryption:

```
E:\archive>"C:\Program Files\WinZip\WZZIP.EXE" -P -s -ycAES256
arc_event_20060401.zip arc_event_20060401

Adding arc_event_20060401\arc_event_data_20060401.dmp
Adding arc_event_20060401\arc_event_data_20060401.exp.log
Adding arc_event_20060401\arc_event_data_20060401_01.dbf
Adding arc_event_20060401\arc_event_data_20060401_02.dbf
Adding arc_event_20060401\arc_event_data_20060401_03.dbf
creating Zip file arc_event_20060401.zip
```

- 3 Generate the SHA1 signature for the archive file `arc_event_20060401.zip` with cygwin's `sha1sum` command:

```
E:\archive>sha1sum arc_event_20060401.zip >
arc_event_20060401.SHA1
```

Example 2: In this example the partition (20060401) archived in the previous example is reactivated. The Archive Directory is `E:\archive`.

- 1 Unzip the archive file `arc_event_20060401.zip` with WinZip command line version to restore the files:

```
E:\archive>"C:\Program Files\WinZip\WZUNZIP.EXE" -d -s
arc_event_20060401.zip
```



```
Zip file: arc_event_20060401.zip
unzipping arc_event_20060401\arc_event_data_20060401.dmp
unzipping arc_event_20060401\arc_event_data_20060401.exp.log
unzipping arc_event_20060401\arc_event_data_20060401_01.dbf
unzipping arc_event_20060401\arc_event_data_20060401_02.dbf
unzipping arc_event_20060401\arc_event_data_20060401_03.dbf
```

- 2 List the contents of the `arc_event_20060401` subdirectory to make sure data files have been extracted:

```
E:\archive>dir arc_event_20060401

Directory of E:\archive\arc_event_20060401

05/09/2006  1,728 arc_event_data_20060401.dmp
05/09/2006   560 arc_event_data_20060401.exp.log
05/09/2006 3,823,657,634 arc_event_data_20060401_01.dbf
05/09/2006 3,657,584,358 arc_event_data_20060401_02.dbf
05/09/2006 3,657,584,287 arc_event_data_20060401_03.dbf
```


Setting up RADIUS User Authentication

This appendix describes how to set up ArcSight Manager to authenticate users using external authentication servers such as the RSA ACE/Server, for authentication using SecurID tokens, instead of the built-in ArcSight authentication mechanism that stores password information in the ArcSight Database. This appendix covers the following topics:

[“Passcodes” on page 159](#)

[“Defining Shorter ArcSight Internal Login User Names” on page 159](#)

[“Two-Factor Challenge Responses” on page 160](#)

[“Steps for Setting Up ACE/Server RADIUS Authentication” on page 161](#)

[“Installing the ACE/Server and ACE/Server RADIUS Service” on page 161](#)

[“Configuring the ACE/Server to allow RADIUS Requests” on page 161](#)

The communication with the RSA ACE/Server works via the RADIUS (Remote Authentication Dial-In User Service) protocol.

Passcodes

When logging in to the ArcSight Console using a SecurID token, type a valid PASSCODE into the Password field. The PASSCODE consists of the PIN and the number displayed on the SecurID token. For example, if the PIN is set to 1234 and the number displayed on the token is 567890, you would type 1234567890 into the Password field.

Defining Shorter ArcSight Internal Login User Names

Often, external authentication systems have user IDs that consist of multiple components (such as the MS Windows domain name and the actual user name). For convenience, you may want to use a shorter name when actually logging in to the ArcSight Console. The following rules apply:

- Every user known to ArcSight Manager has to have a user ID that is unique within ArcSight Manager. This ID will hereafter be referred to as the internal user ID.
- Optionally, another user ID can be specified for each user. This external user ID will be sent to external authentication mechanisms such as the RSA ACE/Server.
- If no external user ID has been provided, the internal user ID will be sent to the external authentication mechanism.

As an example, in ACE/Server, you may have a user account with the user ID eng-jsmith for the user John Smith who works in the engineering group. The user wished to log in to ArcSight Manager using the user ID jsmith. In this case, the external user ID would be set

to eng-jsmith and the internal user ID (and thus the name of the user in ArcSight Manager) would be set to jsmith.

Two-Factor Challenge Responses

If you configured ArcSight Manager to use a RADIUS server connected to a Two-Factor Authentication system such as RSA SecurID for authentication, you will be asked to answer a so-called challenge while authenticating with ArcSight in some cases. Challenges are requests for additional user input that the Two-Factor Authentication server will send to ArcSight during the authentication process.

This challenge mechanism works in the following components of the ArcSight system:

- The ArcSight Console login dialog
- The ArcSight Web login page
- The ArcSight SmartConnector registration wizard
- The ArcSight Manager configuration wizard

Typically, such challenges can include:

- A prompt to enter a new password or PIN code; this request can occur for a number of reasons, for example:
 - ◆ The user is logging in for the first time and has not picked a password/PIN yet.
 - ◆ The password/PIN expired
 - ◆ The requirements for minimum/maximum length of the password/PIN have changed
 - ◆ The authentication system administrator manually initiated a password/PIN change



Note

Make sure that the password/PIN matches the requirements for length and allowed characters as defined in the authentication systems configuration.

- A prompt to wait for the code on the authentication token to change and enter the pass code; this request mostly occurs after changing the password/PIN. Make sure that you enter the pass code, not the token code. Typically, the pass code consists of PIN and token code or of the code that the token displays after entering the PIN (depending on the type of token used).
- A prompt to wait for the code on the authentication token to change and enter the next token code. This request can occur when:
 - ◆ The user has entered a wrong token code for a number of times
 - ◆ The token code the user entered has been used before
 - ◆ The user submitted a token code after the token changed



Note

Wait for the token to change and then code displayed. Do not append the PIN or type the PIN into the token.

Steps for Setting Up ACE/Server RADIUS Authentication

The following is the suggested sequence to set up ArcSight Manager for authentication with ACE/Server.

- 1 Install the ACE/Server and ACE/Server RADIUS service.
- 2 Configure the ACE/Server to allow RADIUS Requests.
- 3 Enable at least one user account to be used with ArcSight Manager in ACE/Server.
- 4 Configure the ArcSight Manager.



Note

Once SecurID authentication is enabled, it is no longer possible to change a user's password or PIN from within the ArcSight Console (the appropriate options are no longer exposed in the user interface). Instead, you need to go through the ACE/Server Database Administration Console to change the PIN of a user.

Installing the ACE/Server and ACE/Server RADIUS Service

Refer to the ACE/Server product documentation for details on this step.



Caution

Before setting up ACE/Server to be accessed by ArcSight Manager, make sure that both the ACE/Server and the ACE/Server RADIUS option are installed and running.

Configuring the ACE/Server to allow RADIUS Requests

Since ArcSight Manager uses RADIUS to authenticate users in ACE/Server, you need to allow the RADIUS service on the ACE/Server to act as a client to ACE/Server. To do this:

- 1 Open the ACE/Server Database Administration Console and select the menu item **Agent Host | Add Agent Host**. Specify entries for the fields as follows:

Name: The host name of the system that is running the ACE/Server.

Agent Type: Communication Server.
- 2 Click **OK** to add the RADIUS service as a client to the ACE/Server.

Next, you need to add the system that is running ArcSight Manager as a client to ACE/Server.
- 3 Again, select **Agent Host | Add Agent Host** from the ACE/Server Database Administration Console and fill in the following fields:

Name: Specify the host name of the system that is running the ArcSight Manager.

Agent Type: Communication Server.
- 4 Click **Assign/Change Encryption Key**.
- 5 Type in a secret.

This secret will be used to encrypt passwords between ArcSight Manager (acting as the RADIUS client) and the RADIUS service portion of ACE/Server (acting as the RADIUS server). You will need to specify it when setting up ArcSight Manager.

- 6 Click **OK** to save the settings.

Enabling User Accounts in ACE/Server

User accounts in ACE/Server need to be activated for the ArcSight Manager host in order to be able to authenticate. To activate a user account:

- 1 In the ACE/Server Database Administration Console menus, select **User | Edit User**.
- 2 Search for the user that you wish to allow access to ArcSight Manager.
- 3 Click **Agent Host Activations**.
- 4 Select the host that runs ArcSight Manager from the "Available Agent Hosts" list on the left hand side, then click **Activate On Agent Hosts**.
- 5 In the dialog, accept the default values by clicking **OK**. Click **Exit** to close the "Agent Host Activations" window and click **OK** again to close the **Edit User** dialog.

Configuring ArcSight Manager

To configure ArcSight Manager for authentication with ACE/Server, you need to run the ArcSight Manager setup tool. This can be done either during the initial installation of ArcSight Manager or afterwards. Either way, to run the ArcSight Manager setup tool, follow these steps:

- 1 Go to the `<ARCSIGHT_HOME>/bin` directory and issue the following command:

```
./arcsight managersetup
```
- 2 Click through the steps as described in [Chapter 3, Installing ArcSight Manager, on page 73](#) until you see a prompt for the authentication method to use.
- 3 Select **RADIUS Authentication** and click the **Next** button.
- 4 Specify entries for following settings:

Authentication Protocol: PAP.

RADIUS Server Host: Specify the host name of the system running ACE/Server. To specify multiple RADIUS servers, enter a comma-separated list of server names in this field.

RADIUS Server Port: Specify the port on which the RADIUS server is running.

RADIUS Shared Secret: Specify the shared RADIUS secret.



The default port for the RADIUS service in SecurID is 1645 and the shared secret is the secret you configured when setting up the Agent Host for ArcSight Manager in ACE/Server.

- 5 Click **Next**.
- 6 On the next panel, you will be asked to provide a user name and password combination. These credentials will only be used to verify that ArcSight Manager can connect to the ACE/Server. Make sure that the user account used has been activated for the ArcSight Manager SmartConnector Host in ACE/Server. For the user name,

enter the ACE/Server user name (i.e. the external user ID) and enter the PASSCODE (based on the PIN and the number on the SecurID token) as the Password.



If this test fails, you will not be able to log into ArcSight Manager.

- 7 If this is the initial setup, make sure to put the correct external user ID into the field in the panel that asks you for the credentials of the new administrator user that will be created.

Migrating from Internal Authentication to ACE/Server

To migrate from internal authentication to ACE/Server authentication, make the changes in the ArcSight Manager setup tool as described in previous setup steps, then log in to the ArcSight Console as an administrator user and change the external IDs for all users (if they differ from internal IDs).



If you are switching from the internal authentication mechanism to ACE/Server after the initial installation and the external user ID of all administrator accounts is different from the internal user ID, contact ArcSight for assistance in setting the external ID for administrator user accounts.

Authentication Troubleshooting

To troubleshoot the communication between ArcSight Manager and ACE/Server and authentication failures, there are three logs that may provide useful information.

- The log written by the ArcSight Manager setup tool, located in `<ARCSIGHT_HOME>\logs\default\serverwizard.log` on the ArcSight Manager system.
- The log written by ACE/Server, available through the ACE/Server Log Monitor tool.
- The debug output from the ACE/Server RADIUS component. It can be enabled using the `rwconfig` tool provided with ACE/Server.

Integrating with iDefense Database

This section describes how to configure your ArcSight Manager so your ArcSight Consoles and ArcSight Web can query the iDefense database.

For information about accessing iDefense information from the Console and ArcSight Web, see each component's online Help.

Configuring Manager for iDefense

To configure your ArcSight Manager to integrate with the iDefense database, follow these steps:

- 1 In `<ARCSIGHT_HOME>\bin`, run this command:

```
arcsight idensesetup
```

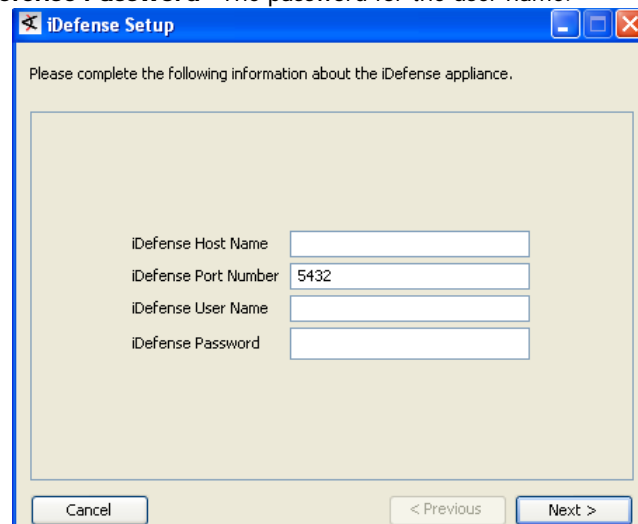
- 2 Enter this information in the wizard that launches:

iDefense Host Name—The machine name of the iDefense system.

iDefense Port Number—The port number on which the Manager should make a connection to the iDefense system.

iDefense User Name—The user name to use to log in to the iDefense system.

iDefense Password—The password for the user name.

A screenshot of the 'iDefense Setup' wizard dialog box. The title bar is blue with the text 'iDefense Setup' and standard window controls. The main area has a light beige background and contains the text 'Please complete the following information about the iDefense appliance.' Below this text are four input fields: 'iDefense Host Name', 'iDefense Port Number' (with '5432' entered), 'iDefense User Name', and 'iDefense Password'. At the bottom of the dialog are three buttons: 'Cancel', '< Previous' (disabled), and 'Next >' (active).

- 3 Click **Next**.

Appendix E

ArcSight Manager Failover

The ArcSight Manager can be set up to work in a high availability (HA) configuration using a third-party failover management (FM) solution. This appendix describes, in general terms, how to configure FM solutions for use with ArcSight Manager and covers the following topics:

[“Architecture” on page 167](#)

[“Starting Processes” on page 169](#)

[“Monitoring Processes” on page 169](#)

[“Next Steps” on page 170](#)

For a detailed description of how to configure a particular product, consult the specific vendor's product documentation.



Please refer to the Deploying ArcSight ESM for High Availability technical note available on the ArcSight Customer Support download site.

Architecture

ArcSight Manager can be deployed as depicted in the figure to achieve high availability. Both the Manager as well as the database can be made highly available. In both cases, it is advisable to have two mostly identical systems. For the database, it is typically preferable to use database-specific FM software.

ArcSight Managers don't use write caches--this means that all writes always immediately go through to the database. They do, however, use read caches. They do not poll the database for changes of the data as it would be too expensive. For this reason, you must not connect two ArcSight Manager instances to the same database at the same time. Otherwise, when one instance updates the database, the objects in the cache of the other instance would become out of date. The object stored in the second Manager's cache would be stale--it would not reflect the most recent update. If then the second Manager changes the stale object and writes it back to the database, the first instance's changes would be lost. If configured properly, the FM software ensures that at any given point in time, there is only a single instance of ArcSight Manager running.

Each of the two systems in a failover group runs an instance of the FM software so that there is no single point of failure. One of the systems is always active; the other one always stands by. The ArcSight Manager software is not running on the standby system. If the FM software detects that the service is no longer running on the active system, it first tries to

restart it and, if that is not possible, fully shuts it down and brings it up on the standby system. At that point in time, the systems switch roles. The system that was formerly the active system becomes the standby system and vice versa.

In order to preserve the state of the rules engine and other state, ArcSight Manager frequently writes this state out to the `<ARCSIGHT_HOME>` directory. In a failover setup, the `<ARCSIGHT_HOME>` should be shared between both instances so that the standby Manager can pick it up upon failover.

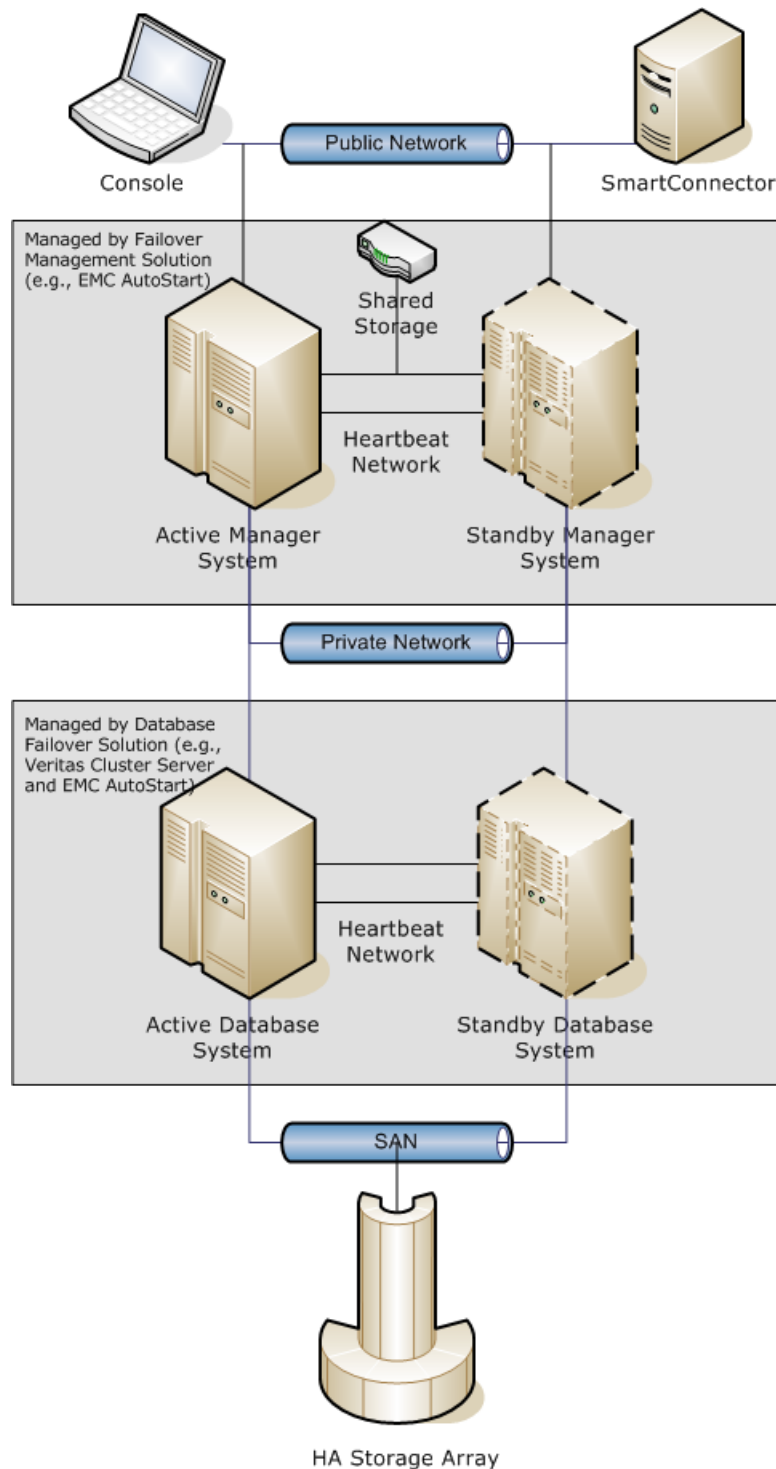


Figure E-1 The ArcSight High Availability (HA) hardware architecture.

To make the failover process transparent to clients, the concept of a virtual IP address is used. (ArcSight SmartConnectors and Consoles are clients of the ArcSight Manager, the ArcSight Manager is a client of the Database.) A virtual IP address is an IP address that is assigned to a system by the FM software. It can be migrated between systems as needed. For example, if the FM software transfers the ArcSight Manager service from one system to another, it moves ArcSight Manager's virtual IP address along with it. Consoles and SmartConnectors simply continue to be able communicate with the Manager through the virtual IP address although it has been moved to another physical system.

In addition to the virtual IP address, each system has at least one other IP address, often referred to as the management IP address. This IP address is used for administrators to communicate with a particular system.

Furthermore, all systems in a group that can host a service should be connected through multiple so-called heartbeat networks. These networks are used by the FM software to communicate the current status of processes. It is crucial that these networks be redundant. If the network fails, it results in a condition often called the "split brain syndrome" - both systems are still up and running, but can no longer communicate. Both systems assume that the other system went down and, as a result, both systems attempt to run the service - leading to undesired and unpredictable results. Many FM software products even provide the ability to set up heartbeat networks using different technologies such as Ethernet and serial cables to get around systemic failures.

Also, all database files as well as the Manager directory need to reside on either shared or real-time replicated storage so they are available to both the active and the stand-by systems at any time. Typically, FM solutions also provide mechanisms to mount and unmount shared storage as needed.

Starting Processes

FM solutions typically use scripts to start up and shut down software components on systems. ArcSight provides simple example scripts in the directory, `<ARCSIGHT_HOME>\utilities\failover`.

These scripts simply call the `\etc\init.d\arcsight_manager` script to start and stop the manager. If you modify these scripts, be careful to shut down processes in the reverse of the order in which they were started.

Monitoring Processes

FM solutions also usually monitor processes using scripts. ArcSight Manager ships with a set of scripts and a small utility that verifies that ArcSight Manager is running and accepting connections. The example scripts can be found under `<ARCSIGHT_HOME>\utilities\failover`. They call `managersetup`, the program which verifies that ArcSight Manager is running and accepting calls. You can also call the program directly by running `runmanagersetup`. This program returns exit code 0 if the Manager is running and reachable, or exit code 1 otherwise.



Caution

This program uses system resources such as CPU cycles and memory (it is a java application) and, if run too often, may negatively influence the overall system performance. The recommended interval is to run this program once a minute. This interval can be configured in the FM software.

Next Steps

After setting up your failover software, test various failure scenarios such as unplugging network cables, power cables, shutting down systems, and so on. Often, the scripts used for FM need to be modified to function reliably in all cases.

Appendix F

FIPS Compliant State Auditing

This appendix covers the following topics:

- [“Compliance State Auditing with Active Channels” on page 171](#)
- [“Compliance State Auditing with Dashboards” on page 172](#)
- [“Compliance State Auditing with Reports” on page 172](#)
- [“Compliance State Auditing with Rules” on page 173](#)

Because ArcSight ESM v4.0.2 supports authentication with both FIPS mode and standard ESM encryption Consoles and SmartConnectors, two new internal audit events have been added to ESM that keep track of non-FIPS component authentications:

- [Found Non FIPS Connector](#) (deviceEventClassID: [authentication:105](#))
- [Found Non FIPS Client](#) (deviceEventClassID: [authentication:202](#))

You can keep track of whether non-FIPs consoles or connectors have authenticated with your FIPS-enabled Manager using one or more of the following features available through the ESM Console.

These methods will list only clients that are not FIPS compliant (running in default mode). If a client is not listed, you can assume that it is FIPS compliant.

- [“Compliance State Auditing with Active Channels” on page 171](#)
- [“Compliance State Auditing with Dashboards” on page 172](#)
- [“Compliance State Auditing with Reports” on page 172](#)
- [“Compliance State Auditing with Rules” on page 173](#)

Compliance State Auditing with Active Channels

Live active channels provide a real-time view of the activity happening on your network currently and in the recent past (such as the last two hours). You can use active channels to view the FIPS compliance status of the hand-shakes occurring between ArcSight components by creating a channel from a filter of ArcSight login events.

To create an active channel from the *ArcSight Login Events* filter:

- 1 In the Navigator, go to [/All Filters/ArcSight Administration/User/](#).
- 2 Right click the *ArcSight Login Events* filter and select **Create Channel with Filter**. This channel shows only events from the past 2 hours with the device event category *Authentication*.

For details about how to work with active channels and edit active channel filters, see the online Help topic *Viewing and Using Channels*.

Compliance State Auditing with Dashboards

Dashboards are a way to see specific views of live events in various graphic forms.

You can build a dashboard made up of data monitors that display non FIPS mode authentications.

To create a data monitor that shows non-FIPS authentications:

- 1** In the Filters area, create a filter that captures one or both of the non-FIPS component events (SmartConnector and Console) described above. You can do this by specifying `Event Name contains FIPS`.
- 2** In the Dashboards section of the Navigator panel, click the Data Monitors tab. Create a new data monitor in an appropriate Data Monitors group, such as Personal, Public, or your user group.
- 3** In the Attributes tab from the *Data Monitor Type* drop-down menu, select an appropriate data monitor type for showing non-FIPS authentications, such as `Hourly Counts` or `Last N Events` and click **Apply**.
- 4** In the Data Monitor attributes fields, enter appropriate values and click **Apply**. For example:
 - a** In the *Name* field, enter a name for the data monitor, such as `Hourly Counts of Non-FIPS Component Authentications` or `Last <15> Non-FIPS Component Authentications`, where <15> is a value you set for how many non-FIPS component authentications you want to see displayed.
 - b** Check the *Enable Data Monitor* checkbox.
 - c** In the *Restrict by Filter* field, select the filter you created above in [Step 1 on page 172](#).
 - d** In the *Field Names* field (if present), select the following two parameters and deselect all others:
 - Event name
 - Device Event Class ID
 - e** Add a description that will help other system users understand the content of the data monitor
 - f** Add any other data monitor attributes you wish this data monitor to display.
- 5** In the Dashboards tab, create a new dashboard, name it appropriately, and add your data monitor to it.
- 6** Repeat steps 2 through 5 to add more FIPS-related data monitors to your dashboard.

For details about how to build dashboards and data monitors, see the online Help topics *Managing Data Monitors* and *Managing Dashboards*.

Compliance State Auditing with Reports

Reports provide captured views or summaries of event data that can be printed or viewed in the ESM Console or ArcSight Web viewer in a variety of formats.

To build a report that shows non-FIPS authentication events:

- 1 In the Reports area of the Navigator panel, click the **Queries** tab. Create a new query that defines one or both of the non-FIPS component authentication events defined in [“FIPS Compliant State Auditing” on page 171](#).
 - a In the *General* tab, name the query appropriately, for example, Non-FIPS Authentications. Add a description, as appropriate, and any other identifying factors desired.
 - b In the *Fields* tab, select the [Event Name](#) and the [Device Event Class ID](#) fields.
 - c In the *Conditions* tab, add a [Matches Filter](#) condition and point to the filter created in [Step 1 on page 172](#) and click **Apply**.
- 2 In the Reports tab, create a new report and add the query you created in [Step 1 on page 173](#).

As an option, you can add a trend for non-FIPS logins over a period of time, for example, the past week.

For details about how to use the reporting tools, see the online Help topics *Building Queries* and *Building Reports*.

Compliance State Auditing with Rules

Rules evaluate incoming events for specific conditions and patterns, then trigger an action in response when a match is found.

You can build rules that, for example, will trigger a notification to alert personnel responsible for the FIPS compliance state of your organization, or populate an active list with any non-FIPS compliant activity, which can be investigated and corrected by your staff.

To build a rule that triggers actions around non-FIPS authentication events:

- 1 In the *Attributes* tab, enter an appropriate name for the rule, for example, one that reflects the conditions it finds and the action(s) it triggers and click **Apply**.
- 2 In the *Conditions* tab, use the Matches Filter condition add a [Matches Filter](#) condition and point to the filter created in [Step 1 on page 172](#) and click **Apply**.
- 3 In the *Aggregation* tab, enter any aggregation parameters relevant to your FIPS auditing situation and click **Apply**.
- 4 In the *Actions* tab, set the thresholds and action(s) you want the rule to trigger when the conditions are met.
- 5 As an option, you can use the *Variables* tab to set additional flexible parameters for the rule.

For details about how to write rules and set notifications, see the online Help topic *Rule Authoring*.

Installing ArcSight ESM in FIPS Mode

This section covers the following topics:

- ["What is FIPS?" on page 175](#)
- ["Network Security Services Database \(NSS DB\)" on page 176](#)
- ["What is PKCS?" on page 176](#)
- ["NSS Tools Used to Configure Components in FIPS Mode" on page 177](#)
- ["TLS Configuration in a Nutshell" on page 177](#)
- ["Using PKCS #11 Token With a FIPS Mode ESM Setup" on page 180](#)
- ["Installing ArcSight Manager in FIPS mode" on page 180](#)
- ["Setting up Partition Archiver in FIPS Mode" on page 187](#)
- ["Installing ArcSight Console in FIPS mode" on page 189](#)
- ["Installing ArcSight Web in FIPS Mode" on page 196](#)
- ["Installing SmartConnectors in FIPS mode" on page 206](#)
- ["How do I Know Whether My Existing ESM Installation is FIPS Enabled?" on page 206](#)
- ["Migrating an Existing Default Mode ESM Installation to FIPS Mode" on page 207](#)



Note

The commands and examples shown are for a Windows system. Path separators are / for Unix and \ for Windows.

Starting in ESM v4.0 SP2, ArcSight ESM supports the Federal Information Processing Standard 140-2(FIPS 140-2). You can choose to install the ESM components in FIPS mode if you have the requirement to do so.



Caution

Before installing ESM in FIPS mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled Manager.

What is FIPS?

FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. A cryptographic module is either a piece of hardware or a software or a combination of the two which is used to implement cryptographic logic. The US Federal government requires

that all IT products dealing with Sensitive, but Unclassified (SBU) information should meet the FIPS 140-2 standard.



Note

To be FIPS 140-2 compliant, you need to have all ESM components configured in the FIPS 140-2 mode. Even though a Manager running in FIPS mode can accept connections from non-FIPS mode components, if you opt for such a mixed configuration, you will not be considered FIPS 140-2 compliant. ArcSight recommends that you run all components in FIPS mode in order to be fully FIPS 140-2 compliant.



Note

- Not all ESM versions or ArcSight Express models support the FIPS mode.
- PKCS #11 token support may not be available for all ESM versions and ArcSight Express models.

Mozilla's Network Security Services (NSS) is an example of FIPS certified cryptographic module. It is the core and only cryptographic module used by ESM in FIPS mode. NSS is an open source security library and collection of security tools. It is FIPS 140-2 compliant and validated. The NSS cryptographic module provides a [PKCS #11](#) interface for secure communication with ESM. You can configure NSS to use either an internal module or the FIPS module. The FIPS module includes a single built-in certificate database token, the [Network Security Services Database \(NSS DB\)](#), which handles both cryptographic operations and the communication with the certificate and key database files.

Network Security Services Database (NSS DB)

A difference between default mode and FIPS mode is that in default mode ArcSight ESM uses the keystore and truststore to store key pairs and certificates respectively in JKS format, whereas in FIPS mode both key pairs and certificates are stored in NSS DB. Key pairs are stored in the .pfx format (in compliance with [PKCS #12](#) standard) in NSS DB. The NSS DB is located in:

- `<ARCSIGHT_HOME>\config\jetty\nssdb` on the Manager
- `<ARCSIGHT_HOME>\current\config\nssdb.client` on the Console
- `<ARCSIGHT_HOME>\config\jetty\webnssdb` on ArcSight Web
- `<ARCSIGHT_HOME>\user\agent\nssdb.client` on ArcSight Database



Note

The default password for the NSS DB on every component is "changeit" without the quotes. However, ArcSight recommends that you change this password by following the procedure in section "Changing the Password for NSS DB" in the *ESM Administrator's Guide*.

What is PKCS?

Public Key Cryptography Standards (PKCS), published by RSA Laboratories, is a group of standards used for reliable and secure public key cryptography. Public Key Cryptography is used to encrypt the data at the sender's end and decrypt 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 or the software that is authorizing the user. ESM uses the PKCS #11 interface provided by the 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.

NSS Tools Used to Configure Components in FIPS Mode

NSS is a cross-platform cryptographic C library and a collection of security tools. ArcSight ESM comes bundled with the following three basic NSS command line tools:

- `runcertutil` - is a certificate and key management tool used to generate key pairs and import and export certificates.



- The `runcertutil` tool currently has a limitation due to which it cannot import the certificate when the NSS DB is set to FIPS mode. To work around this issue, you have to disable FIPS mode in the NSS DB first, then import the certificate, and lastly re-enable FIPS mode.
- When generating a key pair on the Manager or ArcSight Web, it is mandatory to use "mykey" (without quotes) as the alias name for the key pair.

- `runmodutil` - is the NSS module configuration tool. It is used to enable or disable the FIPS module and change Keystore passwords.
- `runpk12util` - is an import and export tool for PKCS #12 format key pairs (.pfx files).

For More information on NSS Tools

See "Appendix A, ArcSight Commands" in the *ArcSight ESM Administrator's Guide* for details on the above command line tools. You can also refer to the 'NSS Security Tools' page on the Mozilla website for more details on any of the above NSS tools (make sure to search for them as certutil, modutil, or pk12util).

For help on any command, enter this command from a component's `\bin` directory:

```
arcisight <command_name> -H
```

TLS Configuration in a Nutshell

TLS configuration involves either server side authentication only or both server side and client side authentication. Setting up client side authentication is optional. To configure ESM in FIPS mode, you need to set up TLS configuration on the Manager, Partition Archiver, Console, and Web.

Since TLS is based on SSL 3.0, we recommend that you have a good understanding of how SSL works. Please read the section “Understanding SSL Authentication” in the *ArcSight ESM Administrator's Guide* for details on how SSL works.

TLS and SSL require the server to have a public/private key pair and a cryptographic certificate linking the server's identity to the public key. The certificate should be signed by an entity that the client trusts. The clients, in turn, should be configured to 'trust' this entity. If the server and clients are controlled by the same authority then certificates can be created locally (self-signed certificates). A more secure approach would be to get the certificate signed by an organization that clients are pre-configured to trust. This involves dealing with one of the many commercial Certification Authorities (CAs).

You have to perform some manual steps to set up the TLS configuration on ESM. This is typically done while installing each component. But, you can also set up the TLS configuration on an existing component.

For detailed instructions on installing a component (fresh installation of the component) in FIPS mode, refer to these sections:

- [“Installing ArcSight Manager in FIPS mode” on page 180](#)
- [“Setting up Partition Archiver in FIPS Mode” on page 187](#)
- [“Installing ArcSight Console in FIPS mode” on page 189](#)
- [“Installing ArcSight Web in FIPS Mode” on page 196](#)

The section, [“Migrating an Existing Default Mode ESM Installation to FIPS Mode” on page 207](#), explains how to convert an existing default mode ESM installation into FIPS mode.

Understanding Server Side Authentication

The first step in an SSL handshake is when the server (Manager) authenticates itself to the client (Console, Web). This is called server side authentication. To set up TLS configuration on your Manager for server side authentication, you need:

- A key pair in your Manager's NSS DB. You can:
 - ◆ Generate a new key pair
 - or
 - ◆ Use an existing key pair.
- The Manager's certificate which incorporates the public key from the key pair located in the Manager's NSS DB. You can use one of the following:
 - ◆ A new self-signed certificate which you generate in the Manager's NSS DB and sign yourself
 - ◆ A new CA-signed certificate which should be imported into the Manager's NSS DB
 - ◆ An existing self-signed or CA-signed certificate which should be imported into the Manager's NSS DB

Next, you should export the Manager's certificate from its NSS DB and lastly import this certificate into the NSS DB of the clients that will be connecting to this Manager. If the Manager has a CA-signed certificate, you have to import the CA's certificate instead of the Manager's CA-signed certificate into the client's NSS DB.

Understanding Client Side Authentication

SSL 3.0 and TLS support client side authentication which you can optionally set up as an extra measure of security. Client side authentication consists of the client authenticating itself to the server. In an SSL handshake, client side authentication, if set up, takes place after the server (Manager) has authenticated itself to the client (Console or Web). At this point, the server requests the client to authenticate itself.

Setting up client side authentication on ArcSight Web is not supported in ESM. Since ArcSight Web is a process within ESM, it does not need to authenticate itself to the Manager.

For the Console to authenticate itself to the Manager, you should have the following in the Console's NSS DB:

- A key pair. You can either:
 - ◆ Generate a new key pair in the Console's NSS DB
 - or
 - ◆ Use an existing key pair which should be imported into the Console's NSS DB
- The Console's certificate which incorporates the Console's public key. You can use one of the following:
 - ◆ a new CA-signed certificate which should be imported into the Console's NSS DB
 - ◆ an existing certificate which should be imported into the Console's NSS DB

Next, you have to export the Console's certificate from its NSS DB and then import it into the NSS DB of the Manager to which the Console will be connecting.

If you plan to use PKCS #11 token such as the Common Access Card, you will be required to import the token's certificate into the Manager's NSS DB as the token is a client to the Manager.

For detailed procedures on each of the steps mentioned above, refer to the appendix, "TLS Configuration to Support FIPS Mode" in the *ArcSight ESM Administrator's Guide*.

Setting up Authentication on ArcSight Web - A Special Case

ArcSight Web plays a dual role. On one hand, it acts as a client to the Manager to which it connects. On the other, it acts as a server to web browsers that connect to it. Therefore, the Web authenticates the Manager but has to authenticate itself to web browsers.

To authenticate the Manager, it should have either the Manager's certificate (if the Manager is using a self-signed certificate) or the certificate of the CA that signed the Manager's certificate (if the Manager is using a CA-signed certificate). So, you should import this certificate into the Web's NSS DB. At the same time, since the Web acts as a server to the web browsers that connect to it, you should have a key pair and the certificate containing the Web's public key in the Web's NSS DB. This allows the Web to authenticate itself to the web browsers.

In a nutshell, you have to:

- Import the Manager's certificate (in the case of self-signed certificate on the Manager) or the certificate of the CA that signed the Manager's certificate (in the case where Manager is using a CA-signed certificate) into the Web's NSS DB.

- Have a key pair in the Web's NSS DB. You can either:
 - ◆ Generate a new key pair
 - or
 - ◆ Use an existing key pair which should be exported in .pfx format and imported into the Web's NSS DB
- Have a Web's certificate containing its public key in the Web's NSS DB. You can use one of the following:
 - ◆ A new self-signed certificate which you generate in the Web's NSS DB and sign yourself
 - ◆ A new CA-signed certificate which needs to be imported into the Web's NSS DB
 - ◆ An existing self-signed or CA-signed certificate which needs to be imported into the Web's NSS DB

The web browsers that try to connect to ArcSight Web import the Web's certificate into their truststore and use it to trust the webserver.

This chapter instructs you on how to set up server-side authentication on ESM. The Manager and Web will be set up using self-signed certificate. For information on setting up client-side authentication or using a CA-signed certificate see the *ESM Administrator's Guide*.

Using PKCS #11 Token With a FIPS Mode ESM Setup

If you plan to use a PKCS #11 Token, such as the ActivClient's Common Access Card (CAC), with this ESM setup that you will be installing by following the procedures in the next few sections, you need to do the steps outlined below in this section.

For details on any of the steps below, see [Appendix H, Using the PKCS#11 Token, on page 217](#).

- 1 Install the CAC provider's software on the machine on which you will be using CAC. For example, if you plan to use CAC with the Console, then install the CAC provider's software on the machine on which you will be installing the Console. The same goes for ArcSight Web.
- 2 Export the CAC card's certificate from the card.
- 3 Extract the root CA's certificate from the CAC card's certificate.
- 4 Copy the root CA's certificate on to the machine(s) on which you plan to install the Console and Web.

Installing ArcSight Manager in FIPS mode

ArcSight Manager requires that the ArcSight Database be installed prior to installing the Manager.

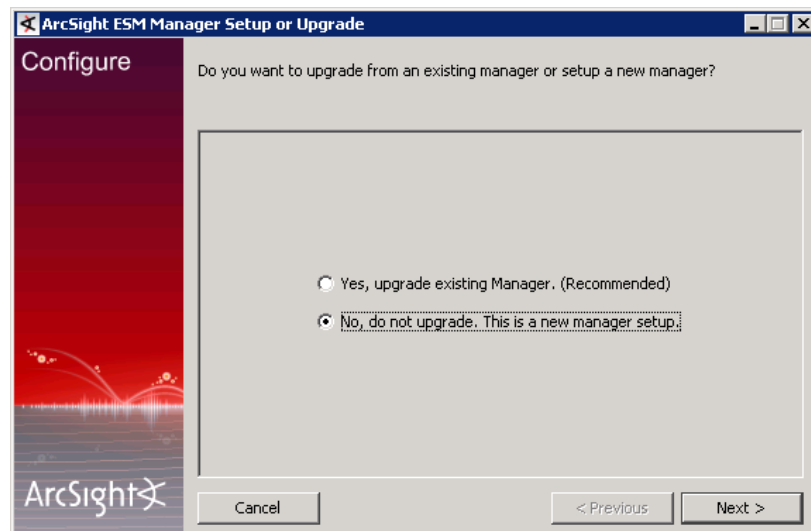
This section instructs you on installing the Manager in FIPS mode only. For steps to install the Manager in default mode, refer to the chapter, ["Installing ArcSight Manager" on page 73](#) or the ArcSight ESM Product Lifecycle document available on the ArcSight Customer Support website. The [Installing ArcSight Manager](#) chapter also lists the supported platforms for ArcSight Manager and contains information that is common to both FIPS mode and default mode.

This section walks you through steps to generate and use a self-signed certificate. If using a CA-signed certificate, see the section, "Using a Certificate Authority (CA) Signed

Certificate” in the *ArcSight ESM Administrator's Guide* for details on obtaining and using a CA-signed certificate.

To install the Manager:

- 1 Create an ArcSight user, usually named 'arcsight,' to own the installation.
- 2 Log in as the ArcSight user before running the Manager Installation Wizard.
- 3 Run the self-extracting archive file that is appropriate for your target platform. See the [Installing ArcSight Manager](#) chapter for information on supported platforms' installation files.
- 4 Follow the prompts in the wizard screens. Refer to [Installing ArcSight Manager](#) chapter for details on each screen.
- 5 When you get to the first configuration screen as shown below, leave the wizard running:



- 6 Open a shell/command prompt window.
- 7 Generate a key pair on the Manager. This key pair is used to generate the self-signed certificate. The self-signed certificate automatically gets generated when you generate the key pair.

The Manager's key pair and certificate get generated and stored in its `nssdb`. The Manager's public key is embedded in its certificate, thereby linking the Manager's identity to its public key.



Note

- If you already have a key pair that you would like to use, you need not generate a key pair. Instead, you can import your existing key pair into the Manager's `<ARCSIGHT_HOME>\config\jetty\nssdb`.
This key pair should be exported in `.pfx` format and then imported into the Manager's NSS DB. Refer to the section, "Using Keytoolgui to Export a Key pair," in the *ArcSight ESM Administrator's Guide* for details on exporting a key pair.
Refer to the section, "Importing an Existing Key pair into the Manager's NSS DB" in the *ArcSight ESM Administrator's Guide* for detailed steps on doing this.
- When you import or generate a key pair into `nssdb`, if there is a existing key pair/certificate that has the same Common Name (CN) as the one you create, the `runcertutil` utility will use the alias of the existing key pair for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

- a** Run the following command from the Manager's `<ARCSIGHT_HOME>\bin` directory to generate a key pair. This will automatically generate the Manager's certificate.

If you want to set the expiry date of the certificate, you have to do so when generating the key pair. Once you have generated the key pair, you cannot change the expiry date on the certificate.



Caution

- Make sure to use "mykey" (without quotes) as the alias name for the key pair as shown in the example.
- The `-m` serial number should be unique within `nssdb`
- Using `-v` is optional. If you choose to use it, see "Setting the Expiration Date of a Certificate" section in the *ArcSight ESM Administrator's Guide* for details.

```
arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey
-k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>\config\jetty\nssdb
```



Caution

For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.

where the hostname is the name of the machine on which your Manager is installed and `-v` is the validity period of the certificate.

When prompted for password, enter "changeit" (without the quotes).

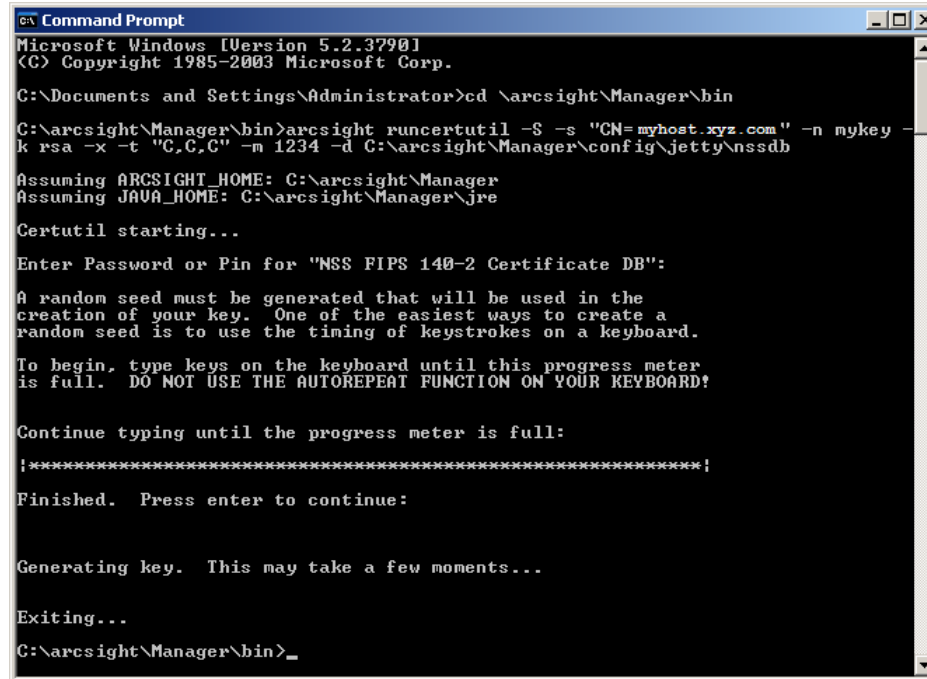
Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key

For example, if your hostname is myhost.arcsight.com, you would run:

```
arcsight runcertutil -S -s "CN=myhost.arcsight.com" -v 6 -n
mykey -k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>\config\jetty\nssdb
```

Using `-v` is optional. If you do not use this option, the certificate will be valid for 3 months by default.

This will generate a key pair and certificate with the alias `mykey` which is valid for 6 months from the current date and time in the Manager's `nssdb`.



```

C:\Documents and Settings\Administrator>cd \arcsight\Manager\bin
C:\arcsight\Manager\bin>arcsight runcertutil -S -s "CN=myhost.xyz.com" -n mykey -
k rsa -x -t "C,C,C" -m 1234 -d C:\arcsight\Manager\config\jetty\nssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre
Certutil starting...
Enter Password or Pin for "NSS FIPS 140-2 Certificate DB":
A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!
Continue typing until the progress meter is full:
|*****|
Finished. Press enter to continue:
Generating key. This may take a few moments...
Exiting...
C:\arcsight\Manager\bin>_

```

- b** To check whether the key pair has been successfully created in the `nssdb`, run the following from the Manager's `<ARCSIGHT_HOME>\bin` directory:

```
arcsight runcertutil -L -d
<ARCSIGHT_HOME>\config\jetty\nssdb
```



```

C:\arcsight\Manager\bin>arcsight runcertutil -L -d C:\arcsight\Manager\config\je
tty\nssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre
Certutil starting...
mykey
Exiting...
C:\arcsight\Manager\bin>_

```

- 8** Export the Manager's certificate.

You are required to have this exported certificate handy when installing the clients (Console and/or Web) that will be connecting to this Manager. You have to import this certificate into the clients' NSS DB

(`<ARCSIGHT_HOME>\current\config\nssdb.client` in case of the Console and `<ARCSIGHT_HOME>\config\jetty\webnssdb` in case of ArcSight Web) when installing them. Importing the Manager's certificate allows the clients to trust the Manager.

To export the Manager's certificate, run the following command from the Manager's `<ARCSIGHT_HOME>\bin` directory:

```
arcsight runcertutil -L -n <certificate_alias> -r -d
<ARCSIGHT_HOME>\config\jetty\nssdb -o <absolute_path_to
_managercertificatename.cert>
```



If you do not specify the absolute path to `managerkey.cer` file destination, the `managerkey.cer` file will be exported to your `<ARCSIGHT_HOME>` directory by default.

For example, to export the certificate as a file named `managerkey.cer` to `C:\arcsight\Manager` directory, run:

```
arcsight runcertutil -L -n mykey -r -d
<ARCSIGHT_HOME>\config\jetty\nssdb -o
C:\arcsight\Manager\managerkey.cer
```

This will generate the `managerkey.cer` file, the Manager's certificate, in `C:\arcsight\Manager` directory.

```

C:\> Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \arcsight\Manager\bin

C:\arcsight\Manager\bin>arcsight runcertutil -L -n mykey -r -d C:\arcsight\Manager\config\jetty\nssdb -o C:\arcsight\Manager\managerkey.cer

Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre
Certutil starting...

Exiting...

C:\arcsight\Manager\bin>_

```

9 (Only if you plan to use CAC with this ESM setup)

If you plan to use CAC with the Console or Web, you need to import the CAC card's CA's root certificate into the Manager's `nssdb`. To do so:

- a Disable FIPS mode in the Manager's `nssdb` by running this command from the Manager's `\bin` directory:

```
arcsigt runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

- b Import the CAC card signer's root certificate by running:

```
arcsight runcertutil -A -n CACcert -t "CT,C,C" -d
<ARCSIGHT_HOME>\config\jetty\nssdb -i
<absolute_path_to_the_root_certificate>
```

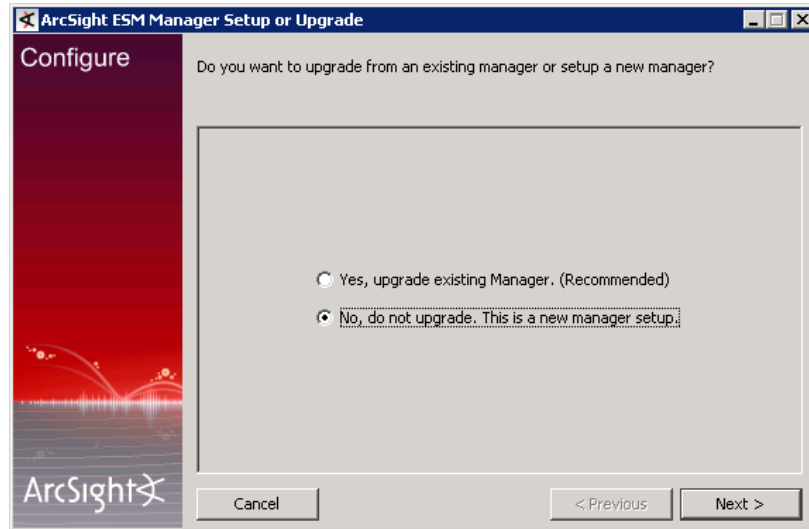


For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

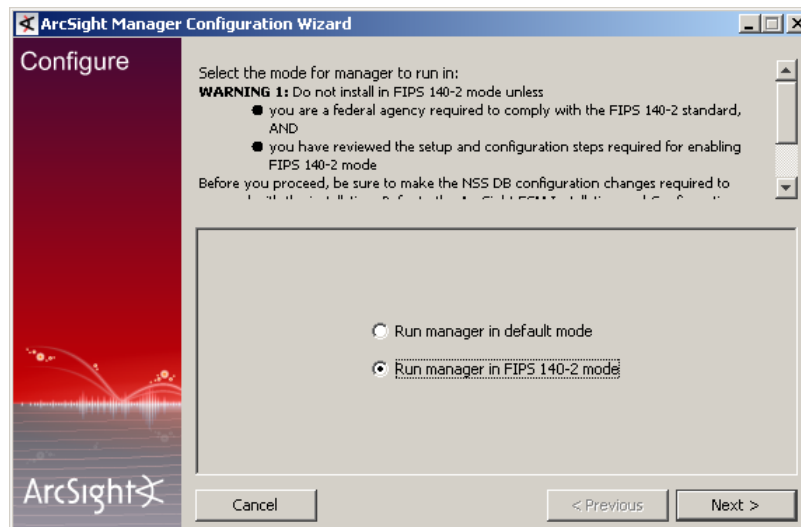
- c Enable FIPS mode in the Manager's `nssdb` by running:

```
arcsigt runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

- 10 Go back to the installation wizard screen and choose **No, do not upgrade. This is a new Manager setup** to create a new, clean installation and click **Next**.

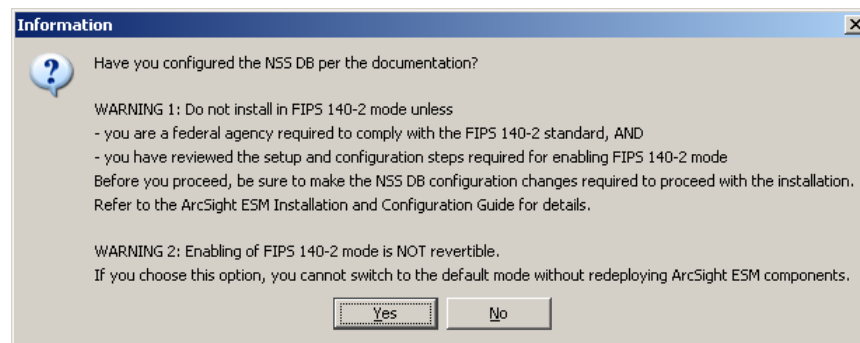


- 11 Next, you will see the following screen:

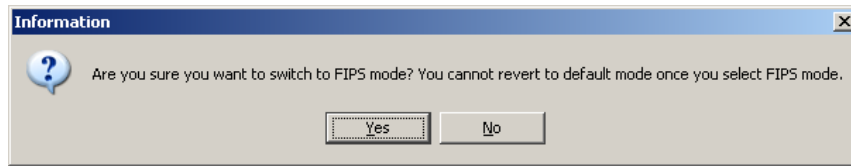


Select the **Run manager in FIPS 140-2 mode** radio button and click **Next**.

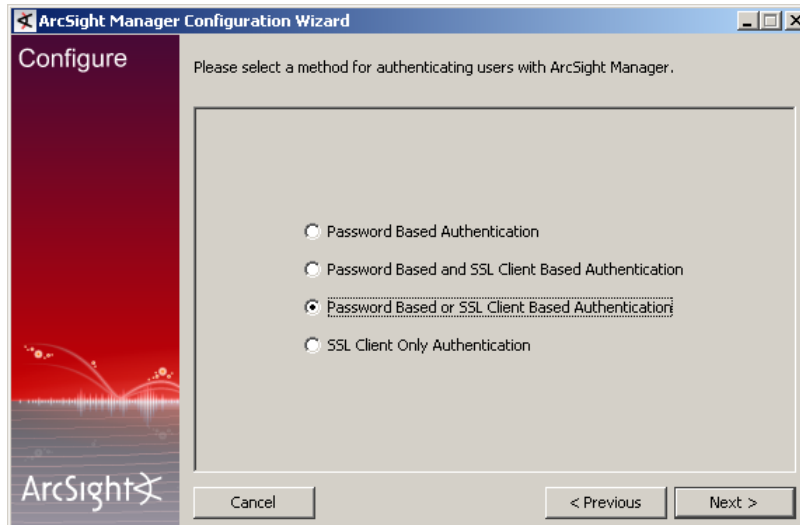
- 12 The configuration wizard will ask you to confirm that you have set up the NSS DB. Click **Yes**.



- 13 You will be reminded that once you select the FIPS 140-2 mode, you will not be able to revert to the default mode. Click **Yes**.



- 14 Follow the prompts in the next few screens until you get to the screen that prompts you to select an authentication setup.



If you do not plan to use CAC with this ESM setup, you can select any option in the screen shown above.

Only if you plan to use CAC with this ESM setup:

- ◆ If you plan to use CAC with Console only:
You can set the authentication option on the Manager to **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication**.
- ◆ If you plan to use CAC with Web only or Web and Console:



Caution

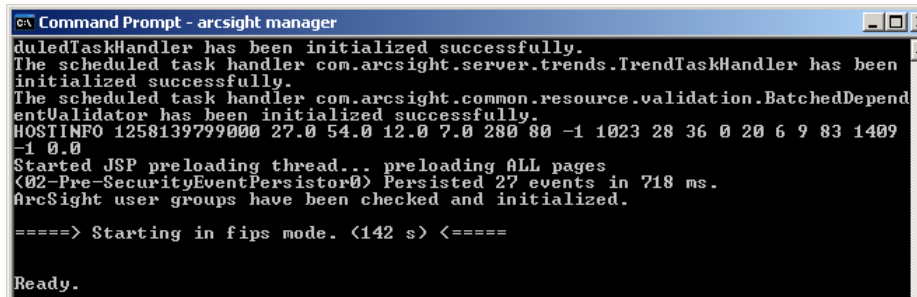
The authentication option you select on the Manager has to match the authentication option on the Web.

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 and set the SSL client keystore to use **PKCS#11 Token**.

- 15 Follow the prompts in the next few wizard screens to complete the Manager installation. Refer to [Installing ArcSight Manager](#) chapter for details on any screen.
- 16 Start the ArcSight Manager by entering the following from the Manager's `\bin` directory:

```
arc sight manager
```

You should see a message that the Manager has started in FIPS mode, as shown in the screenshot below.



```

Command Prompt - arcsight manager
duledTaskHandler has been initialized successfully.
The scheduled task handler com.arcsight.server.trends.TrendTaskHandler has been
initialized successfully.
The scheduled task handler com.arcsight.common.resource.validation.BatchedDependentValidator has been initialized successfully.
HOSTINFO 1258139799000 27.0 54.0 12.0 7.0 280 80 -1 1023 28 36 0 20 6 9 83 1409
-1 0.0
Started JSP preloading thread... preloading ALL pages
<02-Pre-SecurityEventPersistor0> Persisted 27 events in 718 ms.
ArcSight user groups have been checked and initialized.
=====> Starting in fips mode. <142 s> <=====
Ready.

```

Setting up Partition Archiver in FIPS Mode

After the ArcSight Manager has been installed and running, you can optionally configure the Partition Archiver on the ArcSight Database host.

This section outlines the steps for setting up the Partition Archiver in FIPS mode only. Please be sure to read the chapter, [“Installing ArcSight Database” on page 23](#) for other information on Partition Archiver that is common to both the FIPS mode and the default mode.

You must be logged in as the Oracle software owner (by default, 'oracle' on UNIX and Administrator on Windows) to configure Partition Archiver. The wizard will configure Partition Archiver as a standalone application and register it with the ArcSight Manager.

The Partition Archiver is a client to the Manager, so it must be configured to trust the Manager that it will be connecting to. To configure Partition Archiver, you have to import the Manager's certificate into the ArcSight Database's `nssdb.client`. To import the Manager's certificate:

- 1 Open a shell/command prompt window.
- 2 From the database `<ARCSIGHT_HOME>\bin` directory, run the following command to temporarily disable FIPS on the Database's `nssdb.client`:

```

arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\user\agent\nssdb.client

```

Press **Enter** on your keyboard when you see the Warning message.

```

C:\> Command Prompt
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>e:
E:\>cd arcsight\db\bin
E:\arcsight\db\bin>arcsight runmodutil -fips false -dbdir E:\arcsight\db\user\agent\nssdb.client
Assuming ARCSIGHT_HOME: E:\arcsight\db
Assuming JAVA_HOME: E:\arcsight\db\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory E:\arcsight\db\user\agent\nssdb.client...
FIPS mode disabled.

Exiting...
E:\arcsight\db\bin>

```

- 3 Execute the following command to import the Manager's certificate into the Partition Archiver:

```

arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\user\agent\nssdb.client -i
<absolute_path_to_the_manager's_key>

```

```

E:\arcsight\db\bin>arcsight runcertutil -A -n managercert -t "CT,C,C" -d E:\arcsight\db\user\agent\nssdb.client -i C:\arcsight\Manager\managerkey.cer
Assuming ARCSIGHT_HOME: E:\arcsight\db
Assuming JAVA_HOME: E:\arcsight\db\jre
Certutil starting...

Exiting...
E:\arcsight\db\bin>_

```



For the **-t** option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 4 To check whether the Manager's certificate has been imported, run the following command from the Database's **\bin** directory:

```

arcsight runcertutil -L -d
<ARCSIGHT_HOME>\user\agent\nssdb.clinet

```

```

E:\arcsight\db\bin>arcsight runcertutil -L -d E:\arcsight\db\user\agent\nssdb.clinet
Assuming ARCSIGHT_HOME: E:\arcsight\db
Assuming JAVA_HOME: E:\arcsight\db\jre
Certutil starting...

thawtepersonalpremiumca CT,C,C
verisignclass1ca CT,C,C
baltimorecodesigningca CT,C,C
managercert CT,C,C
verisignclass3g2ca CT,C,C
addtrustclass1ca CT,C,C
valicertclass2ca CT,C,C
entrustsslca CT,C,C
thawtepremiumserverca CT,C,C

```

- 5 Run the following command to enable FIPS mode:


```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\user\agent\nssdb.client
```

Press Enter on your keyboard when you see the Warning message.

```
E:\arcsight\db\bin>arcsight runmodutil -fips true -dbdir E:\arcsight\db\user\age
nt\nssdb.client

Assuming ARCSIGHT_HOME: E:\arcsight\db
Assuming JAVA_HOME: E:\arcsight\db\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory E:\arcsight\db\user\agent\nssdb.client...
FIPS mode enabled.

Exiting...

E:\arcsight\db\bin>_
```

- 6 From the ArcSight Database's <ARCSIGHT_HOME>\bin, run the setup program:

```
arcsight agentsetup -w
```

- 7 Select **Run Connector in FIPS 140-2 mode** when prompted.
- 8 Click **OK** when asked whether you have configured the NSS DB.



If you would like to run the `arcsight database pa` command or the `arcsight database pm` command in the remote mode on a Partition Archiver running in FIPS mode, you will have to run these commands from the Manager's <ARCSIGHT_HOME>\bin directory instead of running it from the ArcSight Database's \bin directory.

- 9 Follow the prompts in the next few wizard screens to complete the Partition Archiver set up. Refer to ["Setting Up Partition Archiver" on page 68](#) for details on any screen.

Installing ArcSight Console in FIPS mode



If you would like to set up client-side authentication on the Console, refer to the *ArcSight ESM Administrator's Guide* for details on how to do so.

Install and test the ArcSight Database and Manager before installing the ArcSight Console. Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager and Database hosts.

Refer to the chapter, ["Installing ArcSight Console" on page 109](#) or the ArcSight ESM Product Lifecycle document available on the ArcSight Customer Support website for details on supported platforms for the Console.

This section tells you how to install the Console in FIPS mode only. For details on installing the Console in default mode, refer to the chapter, ["Installing ArcSight Console" on page 109](#). The [Installing ArcSight Console](#) also contains information that is common to both FIPS mode and default mode.

In order for an ArcSight Console to communicate with a FIPS enabled Manager, the Console must trust the Manager. This trust is established by importing the Manager's

certificate into the Console's NSS DB
(`<ARCSIGHT_HOME>\current\config\nssdb.client`).

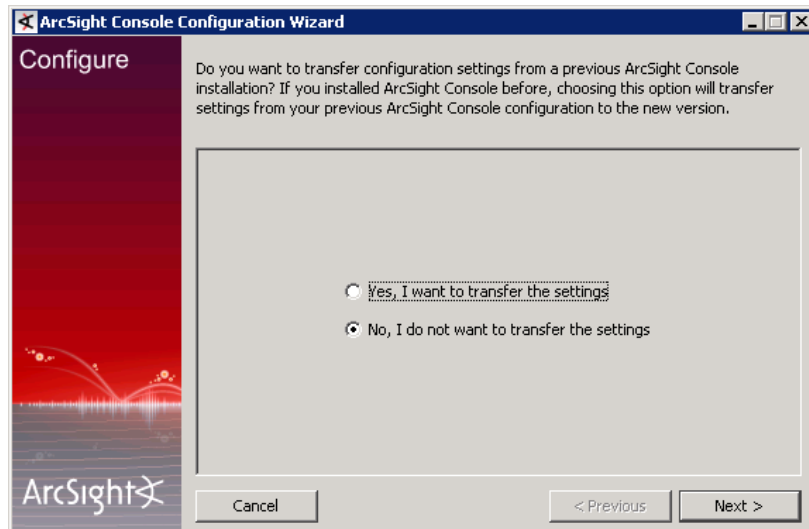


Note

If your Manager is installed on a different machine than the machine on which you will be installing the Console, make sure to copy the Manager's certificate you exported in [Step 8 on page 183](#) to your Console's machine. You are required to import this certificate into the Console's `nssdb.client` when installing the Console.

To install the Console in FIPS mode:

- 1 Run the self-extracting archive file that is appropriate for your target platform.
- 2 Follow the prompts in the wizard screens. Refer to [Installing ArcSight Console](#) chapter for details on each screen.
- 3 When you get to the first configuration screen as shown below, leave the wizard running:



- 4 Open a shell or command prompt window.
- 5 Import the Manager's certificate into the Console's `nssdb.client`.
 - a Set the `nssdb.client` temporarily to non-FIPS 140-2 mode by running the following command from the Console's `<ARCSIGHT_HOME>\current\bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

```

C:\Documents and Settings\ashenoy>cd \arcsight\Console\current\bin
C:\arcsight\Console\current\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Console\current\config\nssdb.client
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode disabled.
Exiting...
C:\arcsight\Console\current\bin>

```

- b** Run the following command to import the Manager's certificate:

```
arcsight runcertutil -A -n managerkey -t "CT,C,C" -d
<ARCSIGHT_HOME>\current\config\nssdb.client -i
<absolute_path_to_managerkey.cert>
```

```

C:\arcsight\Console\current\bin>arcsight runcertutil -A -n managerkey -t "CT,C,C" -d C:\arcsight\Console\current\config\nssdb.client -i C:\arcsight\managerkey.cert
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Certutil starting...
Exiting...
C:\arcsight\Console\current\bin>

```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.



If you do not see any errors, it is an indication that the command ran successfully. You will not see a message saying so.

- c** Run the following command to set the `nssdb.client` back to FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

Press **Enter** on your keyboard when you see the Warning message.

```
C:\arcsight\Console\current\bin>arcsight runmodutil -fips true -dbdir C:\arcsight\Console\current\config\nssdb.client
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode enabled.
Exiting...
C:\arcsight\Console\current\bin>
```

To check whether the certificate has been successfully imported, run the following from the Console's <ARCSIGHT_HOME>\bin directory:

```
arcsight runcertutil -L -d
<ARCSIGHT_HOME>\current\config\nssdb.client
```

```
C:\arcsight\Console\current\bin>arcsight runcertutil -L -d C:\arcsight\Console\current\config\nssdb.client
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Certutil starting...

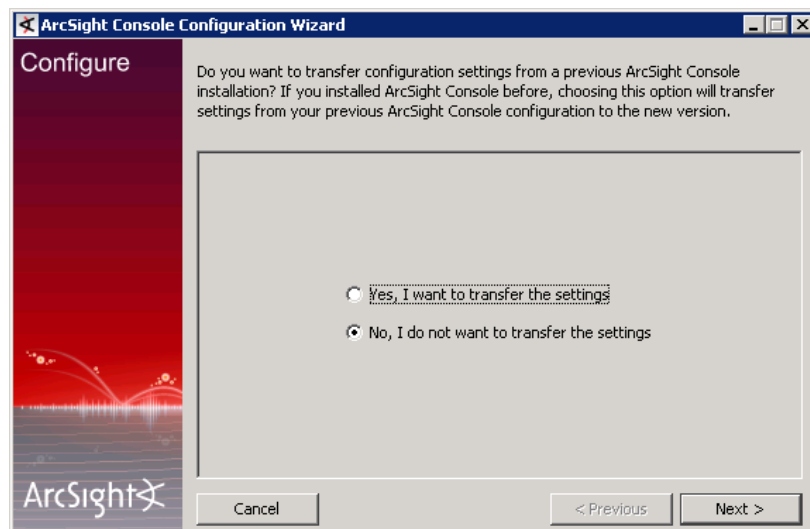
thawtepersonalpremiumca          CT,C,C
verisignclassica                  CT,C,C
halthmorecodesigningca           CT,C,C
managerkey                        CT,C,C
verisignclass3g2ca                CT,C,C
addtrustclassica                  CT,C,C
valicertclass2ca                  CT,C,C
```



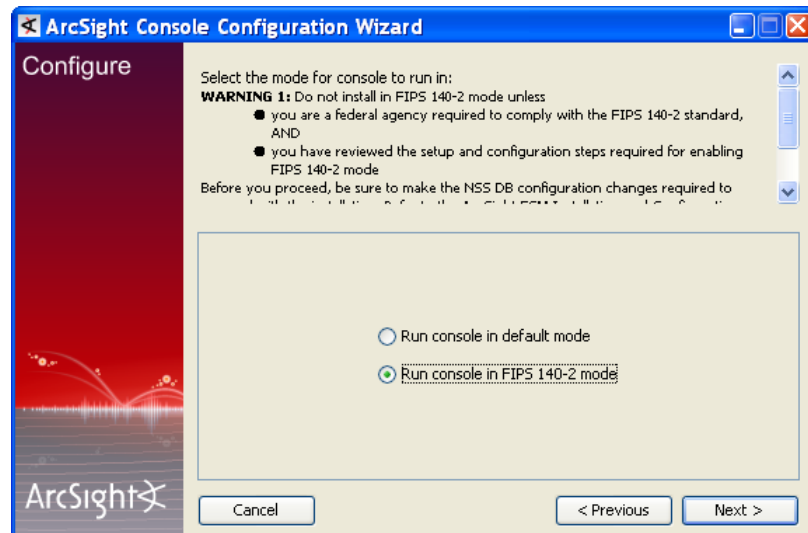
Note

When you import or generate a key pair into NSS DB, if there is a existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility will use the existing alias for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

- 6 Go back to the wizard and select **No, I do not want to transfer the settings** in the following screen and click **Next**:



- 7 Next, you will see the following screen:



Select **Run console in FIPS 140-2 mode** and click **Next**.

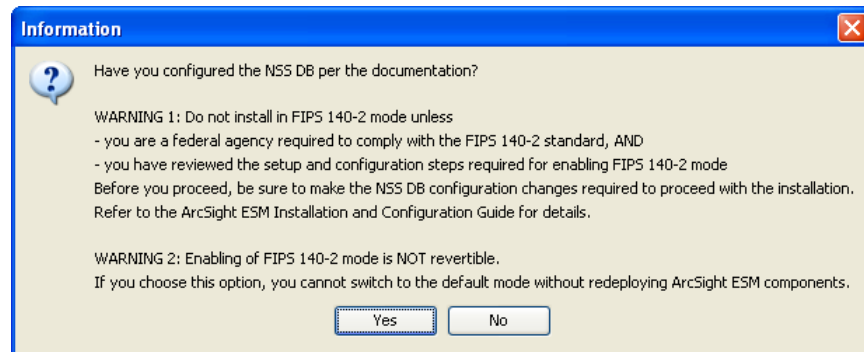


Note

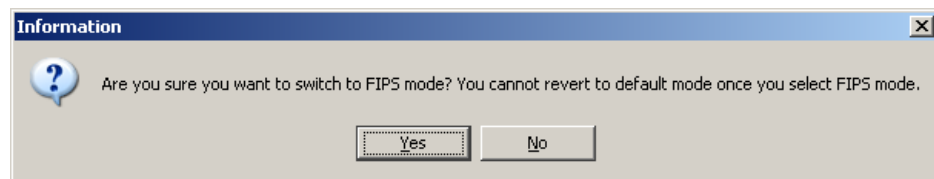
On the Windows XP, SP2 platform, you may see an error asking you to check the certificates in the NSSDB even though you have followed the steps to import the Manager's certificate into the NSSDB successfully. If you encounter this error:

- 1 Either delete or rename the `C:\Windows\system32\nspr4.dll` file.
- 2 Resume your Console installation process by selecting **Run console in FIPS 140-2 mode** and clicking **Next**.

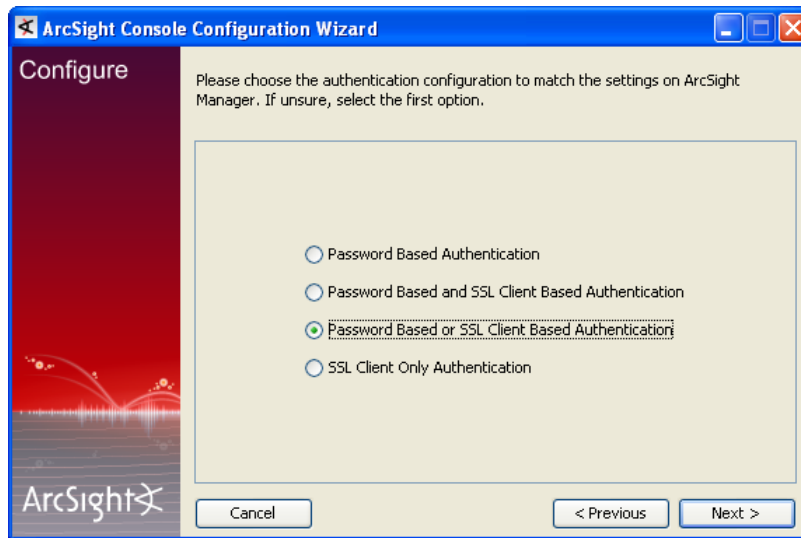
- 8 The configuration wizard will remind you to set up the NSS DB. Click **Yes** in the next dialog.



- 9 You will be reminded that once you select the FIPS 140-2 mode, you will not be able to revert to the default mode. Click **Yes**.



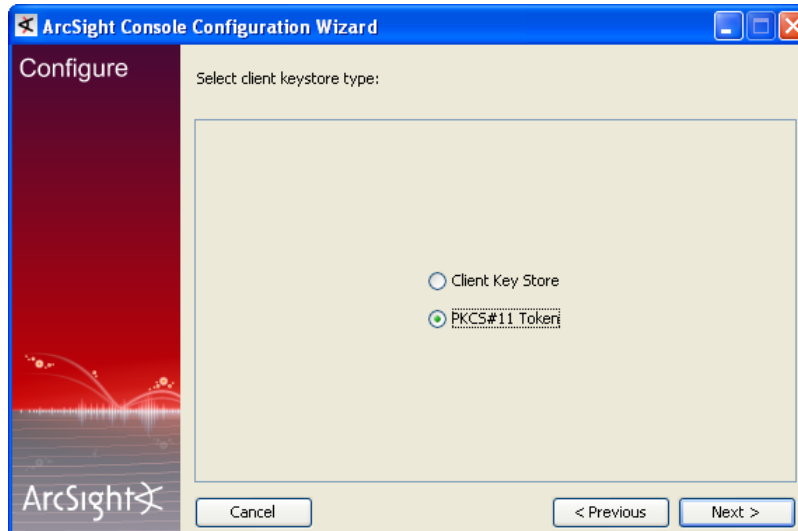
- 10 Follow the prompts in the next few wizard screens until you get to the screen where you have to select the authentication option.



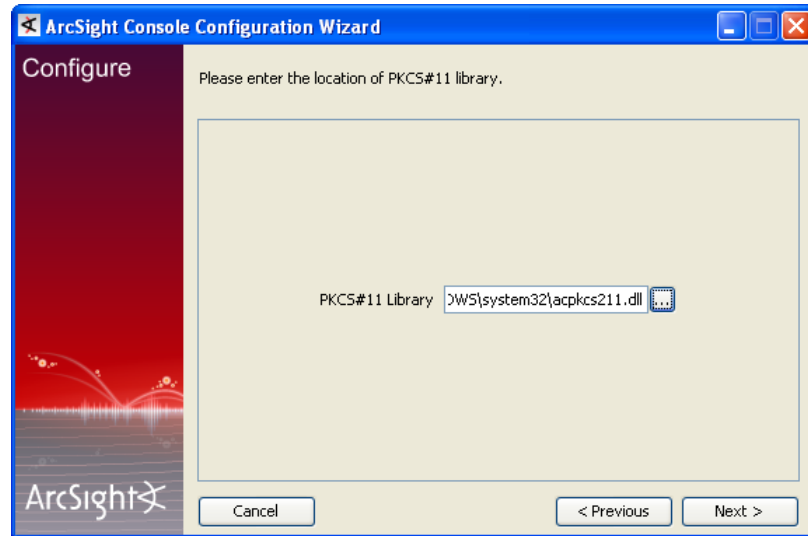
Select the option that you had set on the Manager when installing it.

- 11 If you do not plan to use a PKCS #11 token, select **Client Key Store** in this screen and skip the rest of the instructions in this step and go to the next step.

If you plan to use a PKCS #11 token with the Console, select **PKCS #11 Token** option in the following screen.



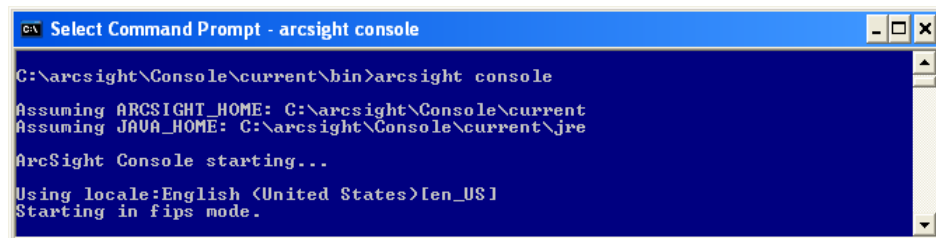
Enter the path or browse to the PKCS #11 library as shown in the following screenshot:



By default, the PKCS #11 library is located in:
[C:\windows\system32\acpkcs211.dll](#).

- 12 Follow the prompts in the next few wizard screens to complete the Console installation. Refer to [Installing ArcSight Console](#) chapter for details on any screen.

When you start the Console, you should see a message saying that the Console is being started in FIPS mode.



Connecting a Default Mode Console to a FIPS Enabled Manager

If you would like to have a Console installed in the default mode to connect to a Manager running in the FIPS 140-2 mode, you will be required to:

- add `server.fips.enabled=true` in your `console.properties` file located in the Console's `<ARCSIGHT_HOME>\current\config` directory.
- add `-Dhttps.protocols=TLSv1` to the `ARCSIGHT_JVM_OPTIONS` variable in the Console's `\current\bin\scripts\console.bat` file.
- import the Manager's certificate into `\current\jre\lib\security\cacerts` on the Console using the `keytoolgui` tool. See section, "Using Keytoolgui to Import a Certificate" in the *ESM Administrator's Guide* for details on how to do this.



Caution

Once you configure your Console running in Default mode to connect to a FIPS enabled Manager by doing the steps above, you will not be able to connect this Console to a Manager running in Default mode without reversing the changes you made to the files.

Connecting a FIPS Enabled Console to Multiple Managers Running in FIPS 140-2 Mode

In order for the Console to connect to multiple Managers running in FIPS 140-2 mode, you will need to do the following:

- 1 For each Manager running in FIPS mode that you want the Console to connect to, import that Manager's certificate into the Console's `nssdb.client`. Refer to [Step 5 on page 190](#) for details on the procedure to do so.



Caution

Make sure that each Manager certificate has a unique Common Name (CN) so that when it is imported it's CN does not conflict with the CN of any existing certificate in the Console's `nssdb.client`.

- 2 If you are using client keystore based SSL client authentication, you also need to import the certificates which coincide with the user on that particular Manager into the Console's `nssdb.client`.

Installing ArcSight Web in FIPS Mode

You can install ArcSight Web on the same host as the ArcSight Manager or on a separate machine that has network access to the Manager. We recommend installing ArcSight Web on a different machine than the Manager.

If you choose to install the ArcSight Web on the same machine as the Manager, when generating a key pair on the Web, set the CN for the Web certificate to be the same as the CN that you used when generating the Manager's certificate.

Install ArcSight Web only after you have installed the ArcSight Manager and have the Manager up and running. You may run multiple instances of ArcSight Web against the same ArcSight Manager, and each instance can be configured with different styling if desired.

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



Note

Make sure that you set any browsers that will be used to connect to ArcSight Web to use the TLS v1 communication protocol. See sections [“Configuring Firefox 3.x to Make it FIPS 140-2 Compliant” on page 203](#) and [“Configuring Internet Explorer to Make it FIPS 140-2 Compliant” on page 206](#) for details on how to do this on Firefox and Internet Explorer respectively.

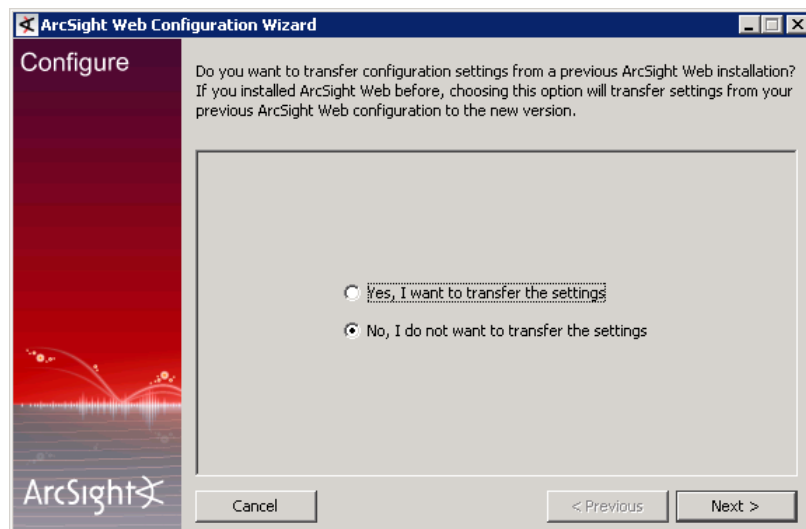
This section instructs you to install the Web in FIPS mode. For details on installing the Web in default mode, refer to the chapter, [“Installing ArcSight Web” on page 129](#). The [Installing ArcSight Web](#) chapter also contains information that is common to both FIPS mode and default mode.

This section walks you through steps to generate a self-signed certificate on the Web. If using a CA-signed certificate, see the section, “Using a Certificate Authority (CA) Signed Certificate” in the *ESM Administrator's Guide* for details on obtaining and using a CA-signed certificate.

The ArcSight Web exposes the Manager's services to the web browser. So, it acts as a server to the web browser but to the Manager, it is a client. As a result, the Web setup is a combination of the Manager setup and the client (Console) setup. In other words, you have to generate a key pair on ArcSight Web (like you do on the Manager) and also import the Manager's certificate into the `webnssdb` (like you do on the Console).

To install and configure ArcSight Web in FIPS mode:

- 1 Run the self-extracting archive file that is appropriate for your target platform. See the [Installing ArcSight Web](#) chapter for information on supported platforms' installation files.
- 2 Follow the prompts in the wizard screens. Refer to [Installing ArcSight Web](#) chapter for details on any screen.
- 3 When you get to the first configuration screen as shown below, leave the wizard running:



- 4 Open a shell/command prompt window.
- 5 Import the Manager's certificate:
 - a Run the following command from ArcSight Web's `<ARCSIGHT_HOME>\bin` directory to temporarily disable the FIPS 140-2 mode:

```
arc sight runmodutil -fips false -dbdir  
<ARCSIGHT_WEB_HOME>\config\jetty\webnssdb
```

Press **Enter** on your keyboard when you see the Warning message.

```

C:\Documents and Settings\ashenoy>cd \arcsight\Web\bin
C:\arcsight\Web\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Web\config\jetty\webnssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Web\config\jetty\webnssdb...
FIPS mode disabled.
Exiting...
C:\arcsight\Web\bin>

```

- b** Run the following command to import the Manager's certificate into ArcSight Web's `webnssdb`:

```

arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t "CT,C,C" -d <ARCSIGHT_HOME>\config\jetty\webnssdb -i <absolute_path_to_managerkey.cer>

```

```

C:\arcsight\Web\bin>arcsight runcertutil -A -n managercert -t "CT,C,C" -d C:\arcsight\Web\config\jetty\webnssdb -i C:\arcsight\managerkey.cer
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Certutil starting...

Exiting...
C:\arcsight\Web\bin>

```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- c** Skip this step if you will not be using CAC with ArcSight Web and go to step d.

Only if you plan to use CAC with Web:

Import the CAC card's CA's root certificate into the Web's `webnssdb`:

```

arcsight runcertutil -A -n CACcert -t "CT,C,C" -d <ARCSIGHT_HOME>\config\jetty\webnssdb -i <absolute_path_to_the_root_certificate>

```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- d** Run the following command to re-enable the FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_WEB_HOME>\config\jetty\webnssdb
```

```
C:\arcsight\Web\bin>arcsight runmodutil -fips true -dbdir C:\arcsight\Web\config\jetty\webnssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Web\config\jetty\webnssdb...
FIPS mode enabled.
Exiting...
C:\arcsight\Web\bin>
```

To check whether the certificate has been successfully imported into the `webnssdb`, run the following from the Web's `<ARCSIGHT_HOME>\bin` directory:

```
arcsight runcertutil -L -d
<ARCSIGHT_HOME>\config\jetty\webnssdb
```

```
Command Prompt
C:\arcsight\Web\bin>arcsight runcertutil -L -d C:\arcsight\Web\config\jetty\webnssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Certutil starting...

thawtepersonalpremiumca CT,C,C
verisignclassica CT,C,C
halmorecodesigningca CT,C,C
managercert CT,C,C
verisignclass3g2ca CT,C,C
addtrustclassica CT,C,C
valicertclass2ca CT,C,C
entrustssica CT,C,C
thawtepremiumserverca CT,C,C
verisignclass2g2ca CT,C,C
entrustglobalclientca CT,C,C
utnuserfirstclientauthenailca CT,C,C
entrust2048ca CT,C,C
```



Note

When you import or generate a key pair into `webnssdb`, if there is a existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility will use the alias of the existing key pair/certificate for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

So, if you install ArcSight Web on the same machine as the Manager, the Manager's certificate will have the same CN as the key pair you generated for ArcSight Web. Hence, the `runcertutil` utility will use the same alias for both the Manager's certificate and the Web's key pair that you generated.

- 6 Generate a key pair on the Web server with an alias `mykey`. This will automatically generate the key pair and the Web's certificate in the `webnssdb`.



Caution

If you have installed ArcSight Web on the same machine as the Manager, make sure to set the CN to be the same as the CN that you used when generating the Manager's certificate.



- If you already have a key pair that you would like to use, you need not generate a key pair. Instead, you can import your existing key pair into the Manager's

`<ARCSIGHT_HOME>\config\jetty\nssdb`.

This key pair should be in `.pfx` format and then imported into the Web's NSS DB. Refer to the section, "Using Keytoolgui to Export a Key pair," in the *ArcSight ESM Administrator's Guide* for details on exporting a key pair.

Refer to the section, "Importing an Existing Key pair into the NSS DB" in the *ArcSight ESM Administrator's Guide* for detailed steps on doing this.

- When you import or generate a key pair into `nssdb`, if there is a existing key pair/certificate that has the same Common Name (CN) as the one you create, the `runcertutil` utility will use the alias of the existing key pair for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

- a** Run the following command from the Web's `<ARCSIGHT_HOME>\bin` directory to generate a key pair. This will automatically generate the Web's certificate.

If you want to set the expiry date for the certificate, you have to do so when generating the key pair. Once you have generated the key pair, you cannot change the expiry date on the certificate.



Caution

- Make sure to use "mykey" (without quotes) as the alias name for the key pair as shown in the example.
- The `-m` serial number should be unique within `webnssdb`
- Using `-v` is optional. If you choose to use it, see "Setting the Expiration Date of a Certificate" section in *ArcSight ESM Administrator's Guide* for details.

```
arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey
-k rsa -x -t "C,C,C" -m 9258 -d
<ARCSIGHT_HOME>\config\jetty\webnssdb
```



Caution

For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.

where the hostname is the name of the machine on which your Web is installed and `-v` is the validity period of the certificate.

- b** Enter the password for `webnssdb`. The default password is 'changeit' (without quotes).
- c** Enter random keyboard strokes when prompted to generate a random seed which will be used to generate your key.

For example, if your hostname is `myhost.arcsight.com`, you would run:

```
arcsight runcertutil -S -s "CN=myhost.arcsight.com" -v 6 -n
mykey -k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>\config\jetty\nssdb
```



For the `-t` option, be sure to use C,C,C protocols only and in the same order that it is shown above.

Use of the `-v` option is optional. If you do not use `-v` to specify a validity period for the certificate, the certificate will be valid for a period of 3 months by default.

This will generate a key pair and certificate with the alias `mykey` which is valid for 6 months from the current date and time in the Web's `webnssdb`

```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ashenoy>cd \arcsight\Web\bin
C:\arcsight\Web\bin>arcsight runcertutil -S -s "CN=myhost.xyz.com" -n mykey -k rs
a -x -t "C,C,C" -m 6543 -d C:\arcsight\Web\config\jetty\webnssdb

Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Certutil starting...
Enter Password or Pin for "NSS FIPS 140-2 Certificate DB":
A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.
To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:
|*****|
Finished. Press enter to continue: .

Generating key. This may take a few moments...

Exiting...
C:\arcsight\Web\bin>

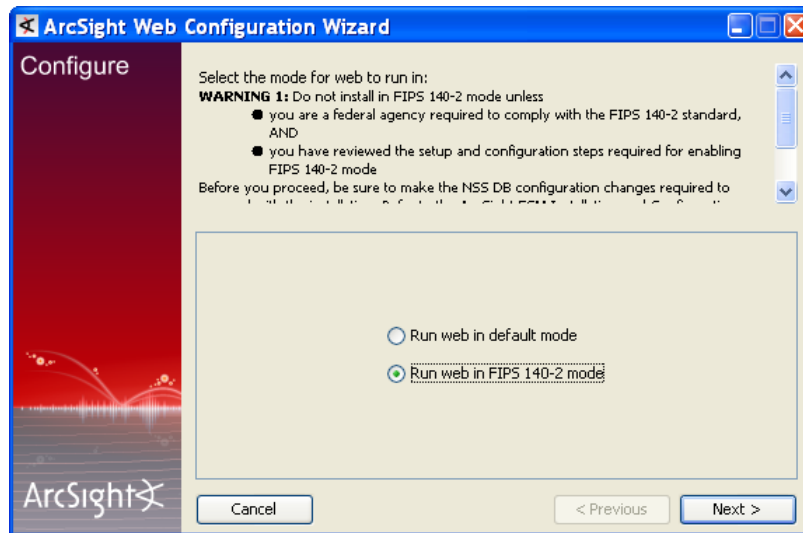
```

To check whether the key pair has been successfully created in the `webnssdb`, run the following from ArcSight Web's `<ARCSIGHT_HOME>\bin` directory:

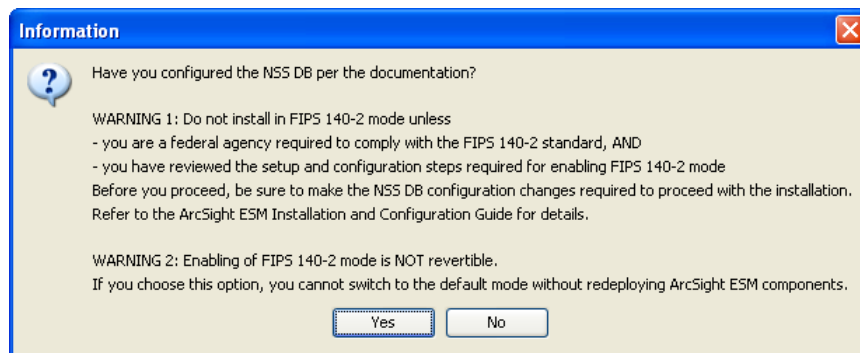
```
arcsight runcertutil -L -d
<ARCSIGHT_WEB_HOME>\config\jetty\webnssdb
```

- 7 Go back to the wizard screen. Select **No, I do not want to transfer the settings** and click **Next**.

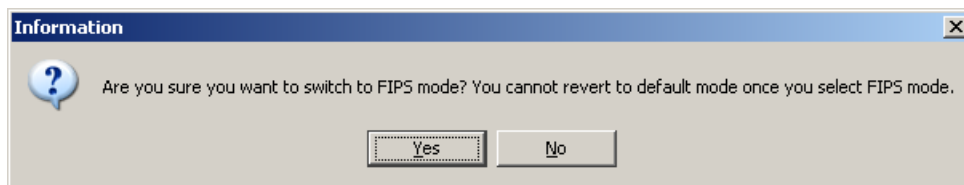
- 8 Select **Run web in FIPS 140-2 mode** in the following screen and click **Next**:



- 9 You will see the following prompt asking you whether you configured your `webnssdb`. Click **Yes**.

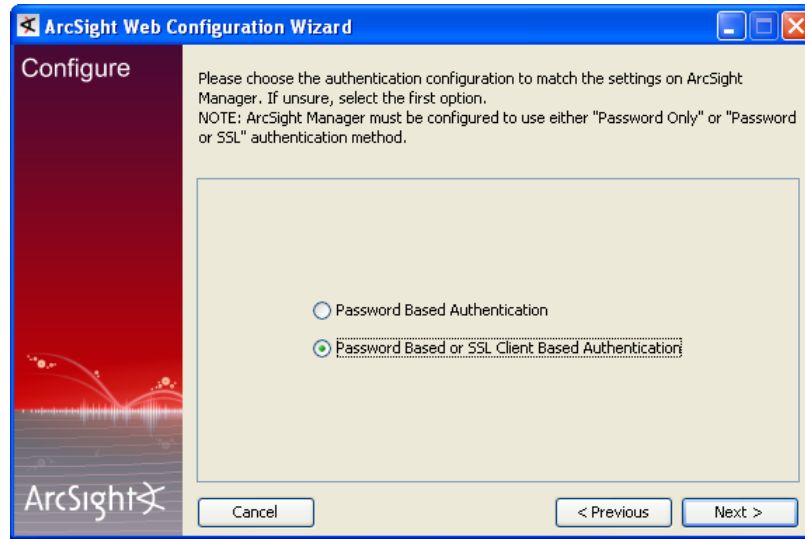


- 10 You will see the following warning:



Click **Yes**.

- 11 Follow the prompts in the next few wizard screens until you get to the screen where you have to select the authentication option on the Web.



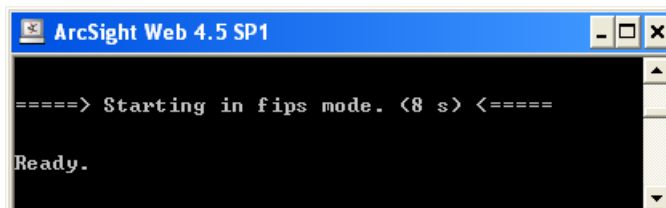
If you do not plan to use CAC with the Web, you can select either of the two options as long as you had set the same option on the Manager when installing it.

If you plan to use CAC with the Web, make sure to select **Password Based or SSL Client Based Authentication**.

- 12 Follow the prompts in the next few wizard screens to complete the ArcSight Web installation. Refer to [Installing ArcSight Web](#) chapter for details on the screens.
- 13 Start ArcSight Web by entering the following from ArcSight Web's `\bin` directory:

```
arcsight webserver
```

You should see a message telling you that the webserver is starting in FIPS mode, as shown below.



- 14 After you have completed installing ArcSight Web in FIPS mode, if you plan to use either Firefox 3.x or the Internet Explorer browser with ArcSight Web, be sure you set your browser to use the TLS v1 communication protocol in order to make them FIPS compliant. Follow the procedures in [Configuring Firefox 3.x to Make it FIPS 140-2 Compliant](#) and [Configuring Internet Explorer to Make it FIPS 140-2 Compliant](#).

Configuring Firefox 3.x to Make it FIPS 140-2 Compliant

If you use Firefox v3.x, you will need to configure it to make it FIPS 140-2 compliant. This section explains how to configure your Firefox v3.x browser for FIPS 140-2 compliance.

- 1 In the Firefox 3.x window, select **Tools->Options...** (or **Edit->Preferences** in the case of Firefox on Linux)
- 2 In the Options window, click the **Advanced** icon.

- 3 Click the **Encryptions** tab to open the page.
- 4 Uncheck the **Use SSL 3.0** check box.
- 5 Check the **Use TLS 1.0** check box.
- 6 Click the **Security Devices** button to open the Device Manager dialog where you will enable FIPS in Firefox's NSS internal PKCS #11 module.
- 7 Click **Software Security Device** and click **Change Password** button.
- 8 Enter a new password and re-enter it to confirm it.
- 9 Select **NSS Internal PKCS #11 Module** and click **Enable FIPS** button.
- 10 Click **OK** to close the Device Manager window and click **OK** to close the Preferences window.
- 11 You must disable all non-FIPS TLS cipher suites. In the location box of the Firefox browser, enter `about:config` and press **Enter**.
- 12 In the message that follows, click the **I'll be careful, I promise** button.
- 13 In the **Filter** textbox, type `ssl`.
- 14 Compare the true/false value for each preference listed on the page that follows with the preference Value in the screenshot below and make sure that the true/false value match the ones shown in the screenshot below. Ignore any additional preferences that

might appear in your browser and not in the screenshot below or vice versa. If any preference value does not match, double click its value to toggle it.

Preference Name	Status	Type	Value
security.enable_ssl2	default	boolean	false
security.enable_ssl3	user set	boolean	false
security.ssl2.des_64	default	boolean	false
security.ssl2.des_ede3_192	default	boolean	false
security.ssl2.rc2_128	default	boolean	false
security.ssl2.rc2_40	default	boolean	false
security.ssl2.rc4_128	default	boolean	false
security.ssl2.rc4_40	default	boolean	false
security.ssl3.dhe_dss_aes_128_sha	default	boolean	true
security.ssl3.dhe_dss_aes_256_sha	default	boolean	true
security.ssl3.dhe_dss_camellia_128_sha	user set	boolean	false
security.ssl3.dhe_dss_camellia_256_sha	user set	boolean	false
security.ssl3.dhe_dss_des_ede3_sha	default	boolean	true
security.ssl3.dhe_dss_des_sha	default	boolean	false
security.ssl3.dhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.dhe_rsa_aes_256_sha	default	boolean	true
security.ssl3.dhe_rsa_camellia_128_sha	user set	boolean	false
security.ssl3.dhe_rsa_camellia_256_sha	user set	boolean	false
security.ssl3.dhe_rsa_des_ede3_sha	default	boolean	true
security.ssl3.dhe_rsa_des_sha	default	boolean	false
security.ssl3.ecdh_ecdsa_aes_128_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_aes_256_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdh_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdh_ecdsa_rc4_128_sha	user set	boolean	false
security.ssl3.ecdh_rsa_aes_128_sha	default	boolean	true
security.ssl3.ecdh_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdh_rsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdh_rsa_null_sha	default	boolean	false
security.ssl3.ecdh_rsa_rc4_128_sha	user set	boolean	false
security.ssl3.ecdhe_ecdsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_null_sha	default	boolean	false
security.ssl3.ecdhe_ecdsa_rc4_128_sha	user set	boolean	false
security.ssl3.ecdhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_rsa_des_ede3_sha	default	boolean	true
security.ssl3.ecdhe_rsa_null_sha	default	boolean	false
security.ssl3.ecdhe_rsa_rc4_128_sha	user set	boolean	false
security.ssl3.rsa_1024_des_cbc_sha	default	boolean	false
security.ssl3.rsa_1024_rc4_56_sha	default	boolean	false
security.ssl3.rsa_aes_128_sha	default	boolean	true
security.ssl3.rsa_aes_256_sha	default	boolean	true
security.ssl3.rsa_camellia_128_sha	user set	boolean	false
security.ssl3.rsa_camellia_256_sha	user set	boolean	false
security.ssl3.rsa_des_ede3_sha	default	boolean	true
security.ssl3.rsa_des_sha	default	boolean	false
security.ssl3.rsa_fips_des_ede3_sha	user set	boolean	false
security.ssl3.rsa_fips_des_sha	default	boolean	false
security.ssl3.rsa_null_md5	default	boolean	false
security.ssl3.rsa_null_sha	default	boolean	false
security.ssl3.rsa_rc2_40_md5	default	boolean	false
security.ssl3.rsa_rc4_128_md5	user set	boolean	false
security.ssl3.rsa_rc4_128_sha	user set	boolean	false
security.ssl3.rsa_rc4_40_md5	default	boolean	false

There is an interoperability issue between Firefox 3.x and Java SSL/TLS server. So, you may see an error in Firefox saying "Can't connect securely because the SSL protocol has been disabled. To resolve this, you will need to disable the TLS Ticket Extension as follows:

- 1 In the location box of the Firefox browser enter `about:config` and press **Enter**.
- 2 In the message that follows, click the **I'll be careful, I promise** button.
- 3 In the **Filter** textbox, enter `TLS`.
- 4 Change the value of `security.enable_tls_session_tickets` preference to `false` by double-clicking it.
- 5 Quit the browser and restart it; then connect to the webserver.

Configuring Internet Explorer to Make it FIPS 140-2 Compliant

Since Internet Explorer is tightly integrated with Windows, you will be required to set up Windows to be FIPS compliant before you configure Internet Explorer itself. To enable FIPS in Windows XP:

- 1 Open **Start->Control Panel->Administrative Tools** and double click **Local Security Policy**.
- 2 Expand the **Local Policies** node in the left pane.
- 3 Click the **Security Options** node.
- 4 In the right pane, double-click **System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** and click the **Enabled** radio button.
- 5 Click **OK**.
- 6 Restart your computer.
- 7 Open the Internet Explorer browser and go to **Tools->Internet Options...**
- 8 Select the **Advanced** tab to open it.
- 9 Select **TLS 1.0** by checking its checkbox.
- 10 Click **OK**.

Installing SmartConnectors in FIPS mode

For information on installing SmartConnectors in FIPS mode see the following documents:

- *Installing FIPS Compliant SmartConnectors*
- *Installing FIPS Compliant Cisco IDS SmartConnectors*
- *Installing FIPS Compliant Sourcefire SmartConnectors*

These documents explain how to install SmartConnectors in FIPS-compliant mode. They are used in conjunction with the individual device SmartConnector configuration guides.

How do I Know Whether My Existing ESM Installation is FIPS Enabled?

To figure out whether your existing installation has been installed in FIPS mode or default mode, check the `fips.enabled` property in the component's property file located in its `<ARCSIGHT_HOME>\config` directory:

- `server.properties` file in the case of Manager
- `console.properties` file in the case of Console
- `webserver.properties` file in the case of ArcSight Web

If FIPS mode is enabled, the property should be set to `fips.enabled=true`. If the component is running in default mode the property will be set to `fips.enabled=false`.

Migrating an Existing Default Mode ESM Installation to FIPS Mode



Before migrating your default mode ESM to FIPS mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled Manager.

To convert an existing default mode ESM installation to FIPS mode, on each component, you have to migrate the existing certificates and key pairs from the component's cacerts and keystore to the component's NSSDB. The following sub-sections provide you step-by-step instructions on how to do so for each component.

Manager

To convert an existing Manager from default mode to FIPS mode:

- 1 Stop the Manager if it is running.
- 2 Export the Manager's key pair from the Manager's `<ARCSIGHT_HOME>\config\jetty\keystore`. Make sure that you export them with a .pfx extension:
 - a Start the keytoolgui by running the following from the Manager's `\bin` directory:


```
arcsight keytoolgui
```
 - b Click **File->Open KeyStore** and navigate to the Manager's `<ARCSIGHT_HOME>\config\jetty\keystore`.
 - c Enter a password for the keystore when prompted. The default password is "changeit" (without quotes).
 - d Right-click the key pair and select **Export**.
 - e Select **Private Key and Certificates** radio button and click **OK**.
 - f Enter the password for the key pair when prompted. The default password is "changeit" (without quotes).
 - g Enter a new password for the key pair file that is about to get exported, then re-enter it to confirm it and click **OK**.
 - h Navigate to the location on your machine to where you want to export the key pair.
 - i Enter `mykey.pfx` as the name for the key pair (make sure to use a .pfx extension) in the Filename textbox and click **Export**.
 - j You will see an Export Successful message. Click **OK**.
- 3 Export the Manager's certificate from the Manager's truststore located in the Manager's `<ARCSIGHT_HOME>\jre\lib\security\cacerts` using the keytoolgui.
 - a Start the keytoolgui by running the following from the Manager's `\bin` directory if it is not already running:


```
arcsight keytoolgui
```
 - b Click **File->Open KeyStore** and navigate to the Manager's `<ARCSIGHT_HOME>\jre\lib\security\cacerts`.

- c Enter a password for the keystore when prompted. The default password is "changeit" (without quotes).
 - d Right-click the Manager's certificate and select **Export**.
 - e Click **OK** in the Export Keystore dialog.
 - f Navigate to the location on your machine to where you want to export the certificate.
 - g Enter a name for the certificate with a .cer extension in the Filename textbox and click **Export**.
 - h You will see an Export Successful message. Click **OK**.
 - i Exit the keytoolgui.
- 4 Set the `nssdb` temporarily to non-FIPS mode by running this command in a command prompt window from the Manager's `<ARCSIGHT_HOME>\bin` directory. (This is a precautionary step to ensure that all FIPS-related processes are disabled before importing certificates into `nssdb`):

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

Press **Enter** on your keyboard when prompted.

```

C:\> Command Prompt

C:\arcsight\Manager\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Manager\config\jetty\nssdb

Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre

Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Manager\config\jetty\nssdb...
FIPS mode disabled.

Exiting...

C:\arcsight\Manager\bin>_

```

- 5 Import the Manager's key pair that you had exported in [Step 2 on page 207](#) into the Manager's `<ARCSIGHT_HOME>\config\jetty\nssdb`. To do so, run the following command from the Manager's `\bin` directory:

```
arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
<ARCSIGHT_HOME>\config\jetty\nssdb
```

Enter the password for the Manager's `nssdb` when prompted. The default password is "changeit" without the quotes.

Enter the password for the .pfx key pair file that you will be importing. This is the password that you set in substep [Step g](#) under [Step 2 on page 207](#).

```

C:\arcsight\Manager\bin>arcsight runpk12util -i C:\arcsight\Manager\mykey.pfx -d
C:\arcsight\Manager\config\jetty\nssdb

Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre

pk12util starting...

Enter Password or Pin for "NSS Certificate DB":
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
C:\arcsight\Manager\bin\nss\win32\pk12util.exe: PKCS12 IMPORT SUCCESSFUL

Exiting...

C:\arcsight\Manager\bin>_

```

- 6 Run the following command from your Manager's `<ARCSIGHT_HOME>\bin` directory to verify that the key pair is imported correctly. Note that the alias of the key pair that you just imported in the `nssdb` will be the same as the alias of that key pair in the `.pfx` file.

```
arcsight runcertutil -L -d <ARCSIGHT_HOME>\config\jetty\nssdb
```

```

C:\arcsight\Manager\bin>arcsight runcertutil -L -d C:\arcsight\Manager\config\je
tty\nssdb

Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre

Certutil starting...

mykey                                u,u,u
Exiting...

C:\arcsight\Manager\bin>_

```

- 7 Import the Manager's certificate that you had exported in [Step 3 on page 207](#) into the Manager's `<ARCSIGHT_HOME>\config\jetty\nssdb`. Run the following command from the Manager's `<ARCSIGHT_HOME>\bin` directory to import the certificate into the Manager's `nssdb`:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\config\jetty\nssdb -i
<absolute_path_to_manager's_certificate>
```

```

C:\arcsight\Manager\bin>arcsight runcertutil -A -n managercert -t "CT,C,C" -d C:
\arcsight\Manager\config\jetty\nssdb -i C:\arcsight\Manager\managercert.cer

Assuming ARCSIGHT_HOME: C:\arcsight\Manager
Assuming JAVA_HOME: C:\arcsight\Manager\jre

Certutil starting...

Exiting...

```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 8 Run the following command to re-enable the FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

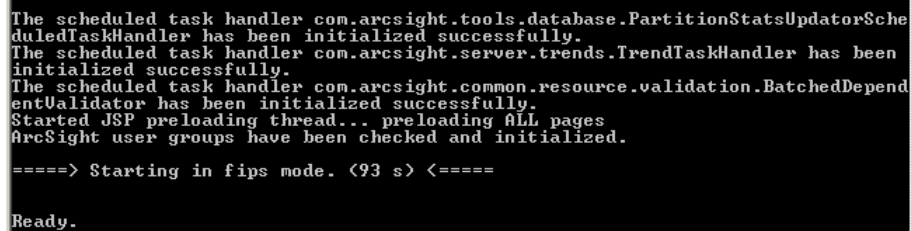
- 9 Run the Manager setup program from the Manager's `\bin` directory:

```
arcsight managersetup
```

- 10 Select **Run Manager in FIPS 140-2 mode**.
- 11 You will receive a reminder asking you to confirm that you have configured the NSS DB. Click **Yes**.
- 12 Follow the prompts in the next few screens until the wizard informs you that you have successfully configured the Manager. Refer to the chapter, "[Installing ArcSight Manager](#)" on page 73 if you need more information on any wizard screen.
- 13 If you had upgraded your Manager from v4.0 SP1 or earlier version, you will also be required to reset all user passwords by running the following command from the Manager's `\bin` directory:

```
arcsight batchresetpwd -f <absolute_path_to_password_file>
```

When you start the Manager, you should see a message telling you that the Manager has started in FIPS mode, as shown in the screenshot below:



```
The scheduled task handler com.arcsight.tools.database.PartitionStatsUpdaterScheduleTaskHandler has been initialized successfully.
The scheduled task handler com.arcsight.server.trends.TrendTaskHandler has been initialized successfully.
The scheduled task handler com.arcsight.common.resource.validation.BatchedDependencyValidator has been initialized successfully.
Started JSP preloading thread... preloading ALL pages
ArcSight user groups have been checked and initialized.

====> Starting in fips mode. <93 s> <====
Ready.
```

Console

To convert an existing Console from default mode to FIPS mode, you will be required to migrate the Manager's certificates from the Console's

`<ARCSIGHT_HOME>\current\jre\lib\security\cacerts` into the Console's `nssdb.client` as described in the procedure below:

- 1 Stop the Console if it is running.
- 2 Export the existing Manager certificate from the Console's `<ARCSIGHT_HOME>\current\jre\lib\security\cacerts` to a location of your choice using the keytoolgui. Refer to the *ArcSight ESM Administrator's Guide* for details on exporting a certificate using keytoolgui.
- 3 If you have client-side authentication configured, you will be required to export the Console's key pair and certificate from the Console's `<ARCSIGHT_HOME>\current\config\keystore.client` as well using keytoolgui. Make sure to export the key pair in .pfx format. Refer to the *ArcSight ESM Administrator's Guide* for details on exporting a certificate using keytoolgui.
- 4 Set the Console's `nssdb.client` temporarily to non-FIPS mode by running the following command from the Console's `<ARCSIGHT_HOME>\current\bin` directory. (This is a precautionary step to ensure that all FIPS-related processes are disabled before importing certificates into `nssdb.client`):

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client
```

```
C:\arcsight\Console\current\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Console\current\config\nssdb.client
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode disabled.
Exiting...
```

- 5 Run the following command from the Console's `<ARCSIGHT_HOME>\current\bin` directory to import the certificate(s) you just exported in the above steps into the Console's `<ARCSIGHT_HOME>\current\config\nssdb.client`. You have to import them one at a time. The screenshot below this command shows you how to import the Manager's certificate only.

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\current\config\nssdb.client -i
<absolute_path_to_certificate's_name>.cer>
```

```
C:\arcsight\Console\current\bin>arcsight runcertutil -A -n managercert -t "CT,C,C" -d C:\arcsight\Console\current\config\nssdb.client -i "C:\Documents and Settings\ashenoy\Desktop\v4.5SP1\managercert.cer"
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Certutil starting...

Exiting...
C:\arcsight\Console\current\bin>
```



Caution

For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

If you had client-side authentication configured, be sure to import the Console's certificate as well from the Console's `cacerts` into its `nssdb.client`.

- 6 If you did not have client-side authentication configured, skip this step.

If you had client-side authentication configured, you will be required to import the Console's key pair into its `nssdb.client`. Run the following from the Console's `\bin` directory:

```
arcsight runpk12util -i <your_file_name.pfx> -d
<ARCSIGHT_HOME>\current\config\nssdb.client
```

- 7 Run the following command to re-enable the FIPS 140-2 mode:


```

arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\current\config\nssdb.client

C:\arcsight\Console\current\bin>arcsight runmodutil -fips true -dbdir C:\arcsight\Console\current\config\nssdb.client
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Console\current\config\nssdb.client...
FIPS mode enabled.
Exiting...
C:\arcsight\Console\current\bin>

```

- 8 Run the Console's setup program by running the following from the Console's `\bin` directory:


```
arcsight consolesetup
```
- 9 Select **No, I do not want to transfer the settings.**
- 10 Select **Run Console in FIPS 140-2 mode.**
- 11 You will receive a reminder asking you to confirm that you have configured the NSS DB. Click **Yes**. You will see another message telling you that you cannot revert to default mode. Click **Yes**.
- 12 Follow the prompts in the next few screens until the wizard informs you that you have successfully configured the Console. Refer to the chapter, "Installing ArcSight Console" on page 109 if you need more information on any wizard screen.

When you start the Console, you should see a message telling you that the Console has started in FIPS mode, as shown in the screenshot below.

```

C:\arcsight\Console\current\bin>arcsight console
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
ArcSight Console starting...
Using locale:English <United States>[en_US]
Starting in fips mode.

```

ArcSight Web

To convert an existing ArcSight Web running in default mode to run in FIPS mode, you have to migrate the Web's key pair, Web's certificate, and the Manager's certificate from the Web's keystore and truststore into its `webnssdb` as outlined in the procedure below.

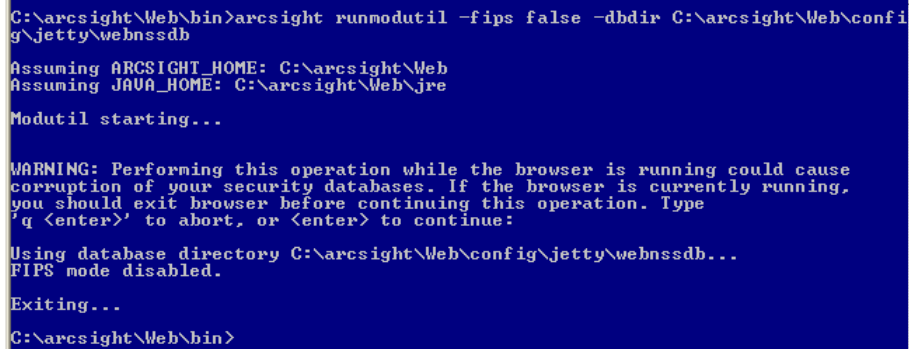
- 1 Stop the Web if it is running.
- 2 Using `keytoolgui`:
 - a Export the Web's key pair from `<ARCSIGHT_HOME>\config\jetty\webkeystore` to a location of your choice. Make sure that you name it `mykey.pfx`. Refer to the *ArcSight ESM Administrator's Guide* for details on using `keytoolgui`.
 - b Export the Web's certificate from the Web's `<ARCSIGHT_HOME>\jre\lib\security\cacerts` to a location of your

choice, using the `keytoolgui`. Refer to the *ArcSight ESM Administrator's Guide* for details on using `keytoolgui`.

- c Export the Manager's certificate from the Web's `<ARCSIGHT_HOME>\jre\lib\security\cacerts` to a location of your choice, using the `keytoolgui`.

- 3 Set the `webnssdb` temporarily to non-FIPS mode by running this command from the Web's `<ARCSIGHT_HOME>\bin` directory. (This is a precautionary step to ensure that all FIPS-related processes are disabled before importing certificates into `webnssdb`):

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\config\jetty\webnssdb
```



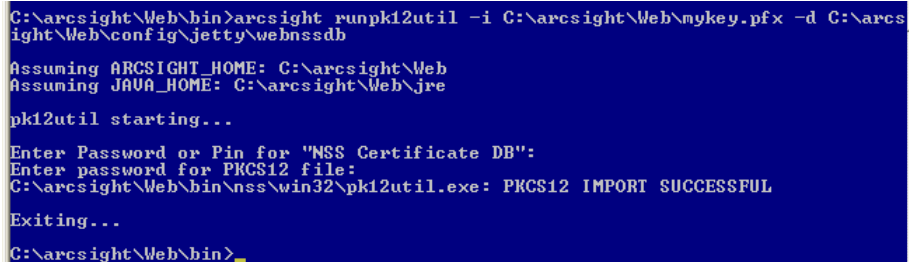
```
C:\arcsight\Web\bin>arcsight runmodutil -fips false -dbdir C:\arcsight\Web\config\jetty\webnssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Web\config\jetty\webnssdb...
FIPS mode disabled.
Exiting...
C:\arcsight\Web\bin>
```

- 4 Import the Web's key pair which you exported in [Step a](#) into its `<ARCSIGHT_HOME>\config\jetty\webnssdb` by running the following command from its `\bin` directory:

```
arcsight runpk12util -i <absolute_path_to_mykey.pfx> -d
<ARCSIGHT_HOME>\config\jetty\webnssdb
```



```
C:\arcsight\Web\bin>arcsight runpk12util -i C:\arcsight\Web\mykey.pfx -d C:\arcsight\Web\config\jetty\webnssdb
Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre
pk12util starting...
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
C:\arcsight\Web\bin\nss\win32\pk12util.exe: PKCS12 IMPORT SUCCESSFUL
Exiting...
C:\arcsight\Web\bin>
```

- 5 Run the following command from your Web's `<ARCSIGHT_HOME>\bin` directory to verify that the key pair is imported correctly. Note that the alias of the key pair that you just imported in the `webnssdb` will be the same as the alias of that key pair in the `.pfx` file.

```
arcsight runcertutil -L -d
<ARCSIGHT_HOME>\config\jetty\webnssdb
```

- 6 Import the Web's certificate which you exported in [Step b](#) into its `<ARCSIGHT_HOME>\config\jetty\webnssdb` by running the following command from its `\bin` directory:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\config\jetty\webnssdb -i
<absolute_path_to_webcertificate>
```

```
C:\arcsight\Web\bin>arcsight runcertutil -A -n webcert -t "CT,C,C" -d C:\arcsight
\Web\config\jetty\webnssdb -i C:\arcsight\Web\webcert.cer

Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre

Certutil starting...

Exiting...

C:\arcsight\Web\bin>_
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 7 Import the Manager's certificate which you exported in [Step c](#) into its `<ARCSIGHT_HOME>\config\jetty\webnssdb` by running the following command from its `\bin` directory:

```
arcsight runcertutil -A -n <provide_an_alias_for_the_cert> -t
"CT,C,C" -d <ARCSIGHT_HOME>\config\jetty\webnssdb -i
<absolute_path_to_manager's_certificate>
```

```
C:\arcsight\Web\bin>arcsight runcertutil -A -n managercert -t "CT,C,C" -d C:\arc
sight\Web\config\jetty\webnssdb -i "C:\Documents and Settings\ashenoy\Desktop\04
.5SPI\managercert.cer"

Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre

Certutil starting...

Exiting...

C:\arcsight\Web\bin>_
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 8 Run the following command to re-enable the FIPS 140-2 mode:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\jetty\webnssdb
```

```
C:\arcsight\Web\bin>arcsight runmodutil -fips true -dbdir C:\arcsight\Web\config
\jetty\webnssdb

Assuming ARCSIGHT_HOME: C:\arcsight\Web
Assuming JAVA_HOME: C:\arcsight\Web\jre

Modutil starting...

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory C:\arcsight\Web\config\jetty\webnssdb...
FIPS mode enabled.

Exiting...

C:\arcsight\Web\bin>
```

- 9 Run the Web's setup program by running the following from the Web's `\bin` directory:

```
arcsight websetup
```

- 10** Select **No, I do not want to transfer the settings.**
- 11** Select **Run web in FIPS 140-2 mode.**
- 12** You will receive a reminder asking you to confirm that you have configured the NSS DB. Click **Yes.**
- 13** Follow the prompts in the next few screens until the wizard informs you that you have successfully configured ArcSight Web. Refer to the chapter, [“Installing ArcSight Web” on page 129](#) if you need more information on any wizard screen.

When you start the webserver, you should see a message saying that the webserver is starting in FIPS mode as shown in the screenshot below.

```
====> Starting in fips mode. (12 s) <====  
  
Ready.
```



Caution

Make sure to set your browser to use TLS. Follow the instructions in [“Configuring Firefox 3.x to Make it FIPS 140-2 Compliant” on page 203](#) if you plan to use Firefox. If you plan to use Internet Explorer, follow the instructions in [“Configuring Internet Explorer to Make it FIPS 140-2 Compliant” on page 206](#).

Appendix H

Using the PKCS#11 Token

This appendix covers the following topics:

[“What is PKCS?” on page 217](#)

[“PKCS#11 Token Support in ESM” on page 218](#)

[“An Example - Using the ActivClient CAC Card” on page 218](#)

[“Using CAC with ArcSight Console” on page 218](#)

[“Using CAC with ArcSight Web” on page 226](#)

Starting ESM v4.0 SP2, 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.



You can use the PKCS#11 token regardless of the mode that the Manager is running in - with Manager running in FIPS 140-2 mode or with Manager running in the default mode.

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 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 ESM

ArcSight ESM 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.

You can use a PKCS#11 token regardless of the mode in which the client is running - you can use it with clients running in FIPS 140-2 mode or with clients running in the default mode. To use a PKCS #11 token with ESM installed in either mode, you have to 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.

An Example - Using the ActivClient CAC Card

Even though ESM 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

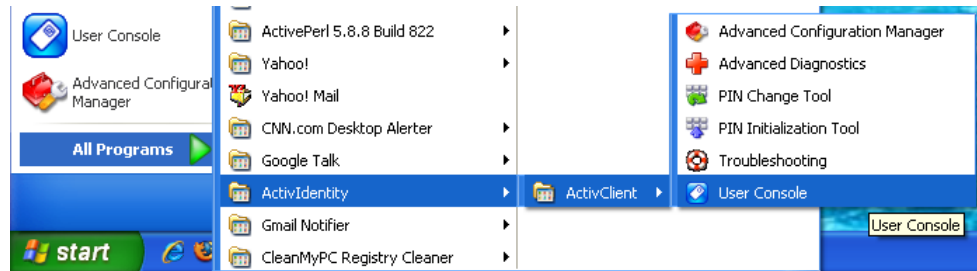
You are required to map the Common Name (CN) on the CAC to a User's External ID on the Manager. This allows the Manager to know which of its user is being represented by the identity stored in the CAC card.



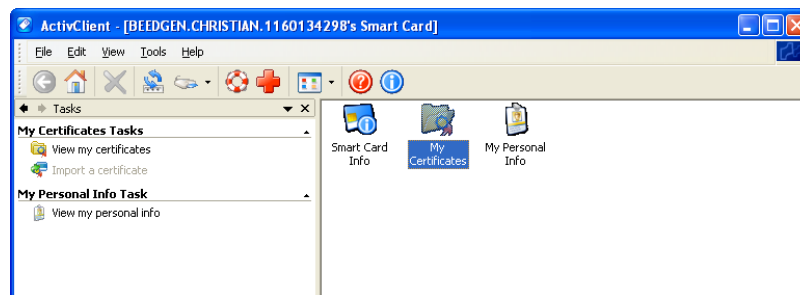
The CAC card contains three types of certificate, Signature, Encryption and ID certificates. Only ID certificate is supported.

- 1 Obtain the Subject CN from the CAC card.

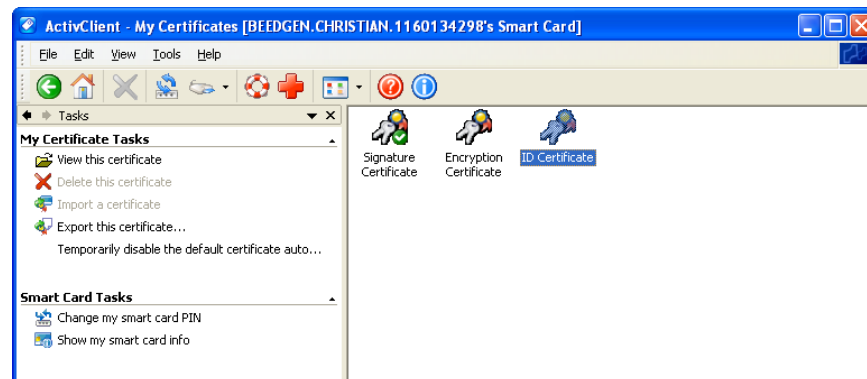
- a Insert the CAC card into the reader if not already inserted.
- b Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



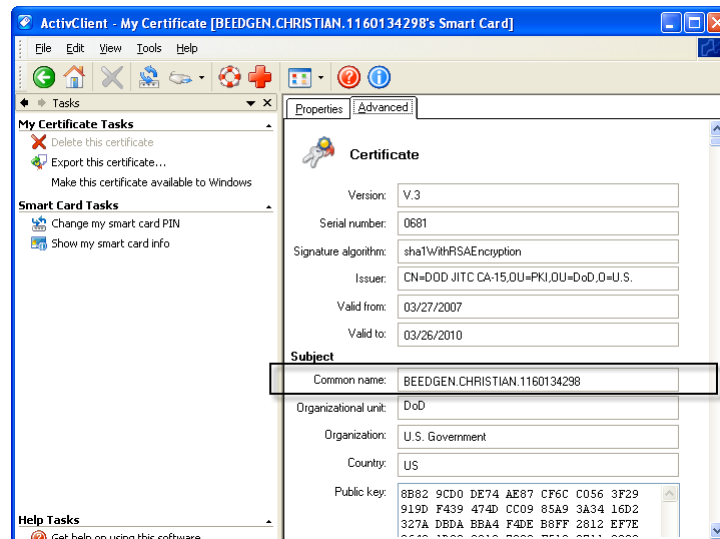
- c Double click **My Certificates** in the following screen:



- 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**.

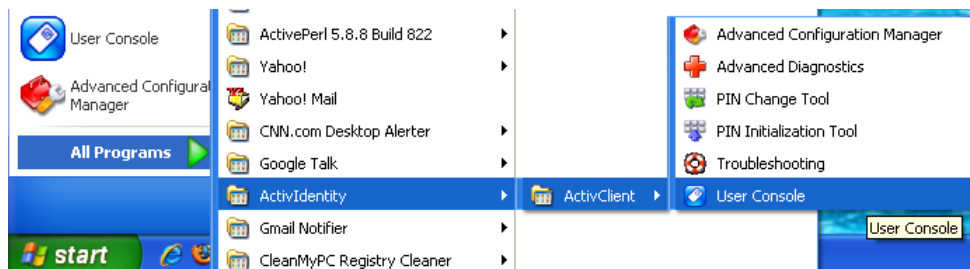
Export the CAC's Certificate

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.

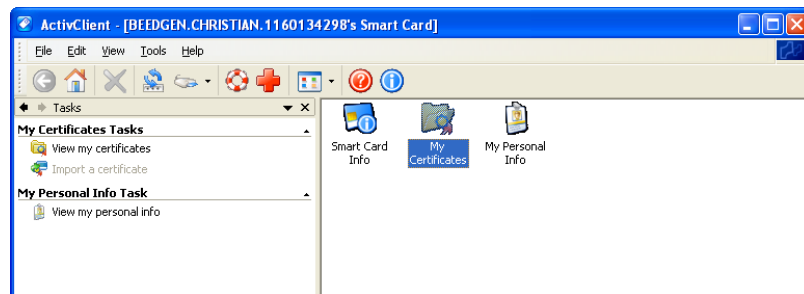
You need to export the CAC's certificate from its truststore. You need this certificate in order to extract the root CA certificate from this certificate.

The steps to do so are:

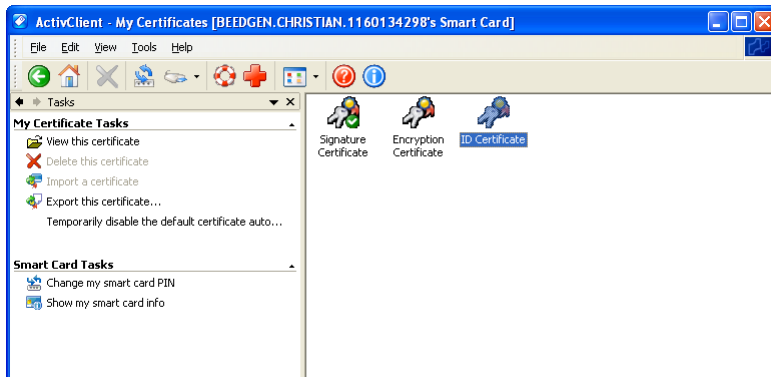
- 1 Insert the CAC card into the reader if not already inserted.
- 2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



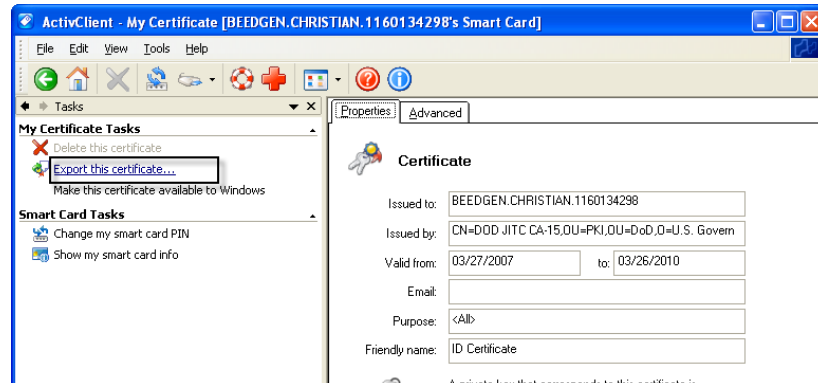
- 3 Double click **My Certificates** in the following screen:



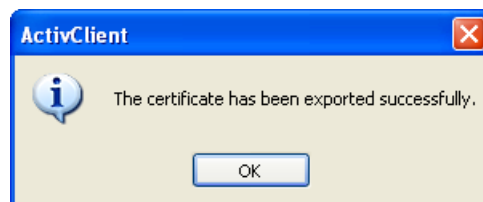
- 4 Double click **ID Certificate** in the following screen:



- 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:

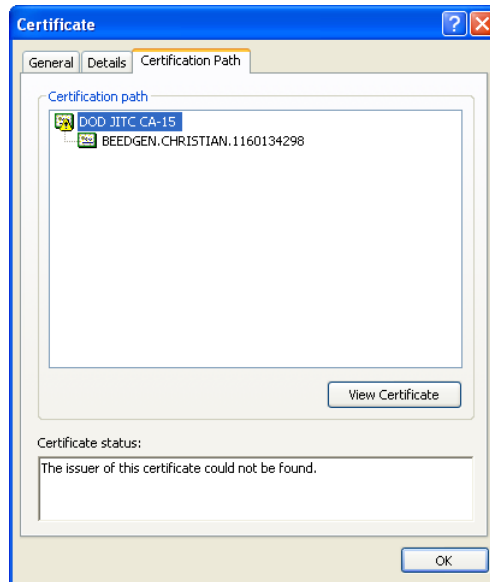


- 8 Exit the ActivClient window.

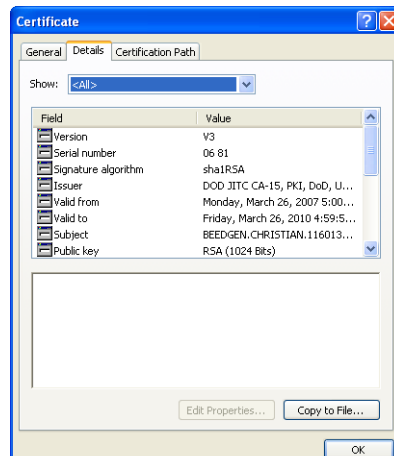
Extract the Root CA Certificate From the CAC Certificate you Exported

This step is required because you are required to import the CAC card certificate signer's 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 the **Details** tab and click **Copy to File...**



- 4 The Certificate Export Wizard will open. Follow the prompts in the wizard screens and accept all the defaults.
- 5 Enter a name for the CAC root 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.
- 6 Exit the Certificate dialog.

Import the CAC Card's Root CA Certificate into the ESM Manager's nssdb

To import the certificate into the Manager's nssdb:

- 1 Stop the Manager if it is running.
- 2 Disable FIPS mode in the Manager's nssdb by running this command from the Manager's \bin directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

- 3 Import the CAC card signer's root certificate by running:

```
arcsight runcertutil -A -n CACcert -t "CT,C,C" -d
<ARCSIGHT_HOME>\config\jetty\nssdb -i
<absolute_path_to_the_root_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 4 Enable FIPS mode in the Manager's nssdb by running:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\jetty\nssdb
```

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.



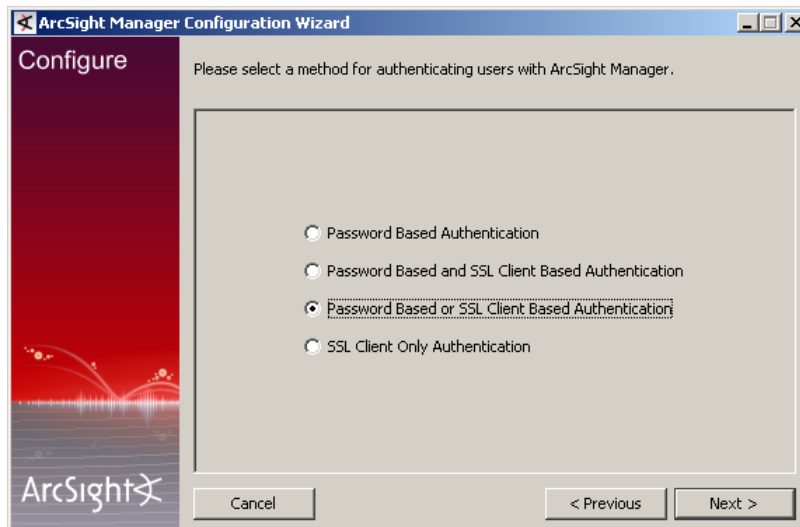
The authentication option you select on the Manager has to match the authentication option on the Web.

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 and set the SSL client keystore to use **PKCS#11 Token**.

To set the authentication option on the Manager:

- 1 Run the Manager's setup program from the Manager's \bin directory:


```
arcsight managersetup
```
- 2 Select **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication** in the following screen.

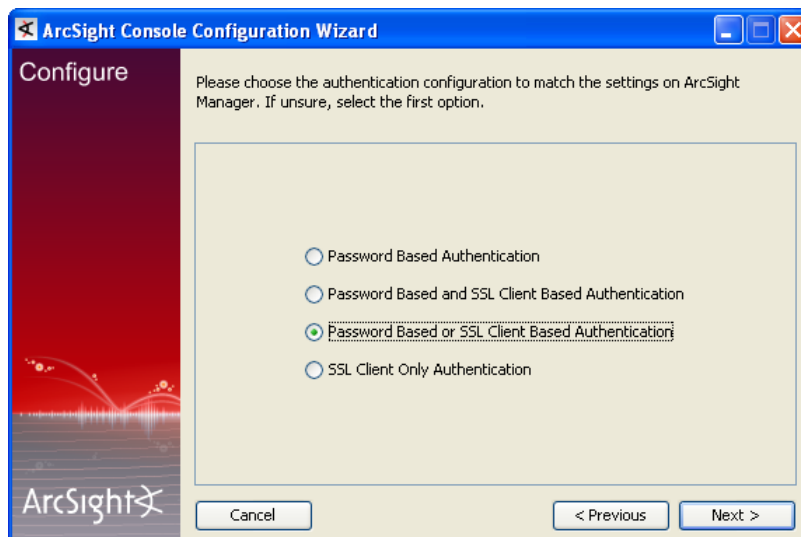


- 3 Complete the setup by following the prompts in the next few screens.
- 4 Start the Manager.

Select Authentication Option in Console Setup

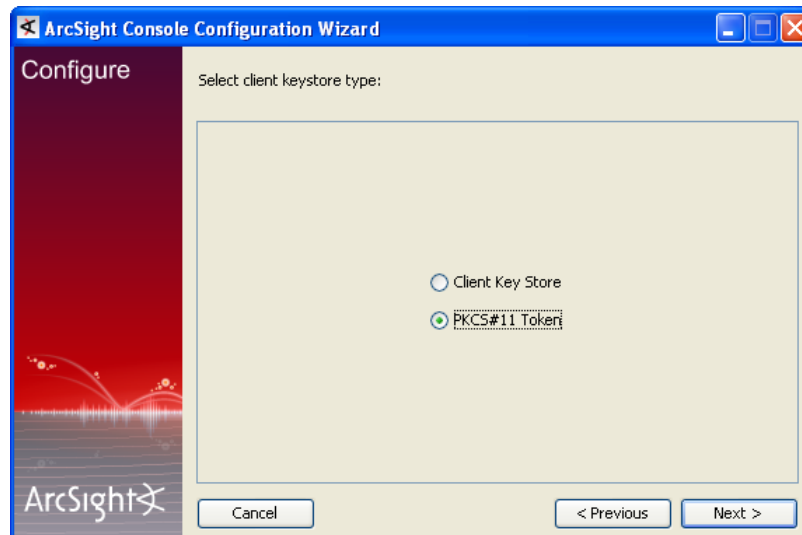
The authentication option on the Console should match the authentication option that you set on the Manager. Run the Console setup program and either confirm or change the authentication on the Console to match that of the Manager. To do so:

- 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.

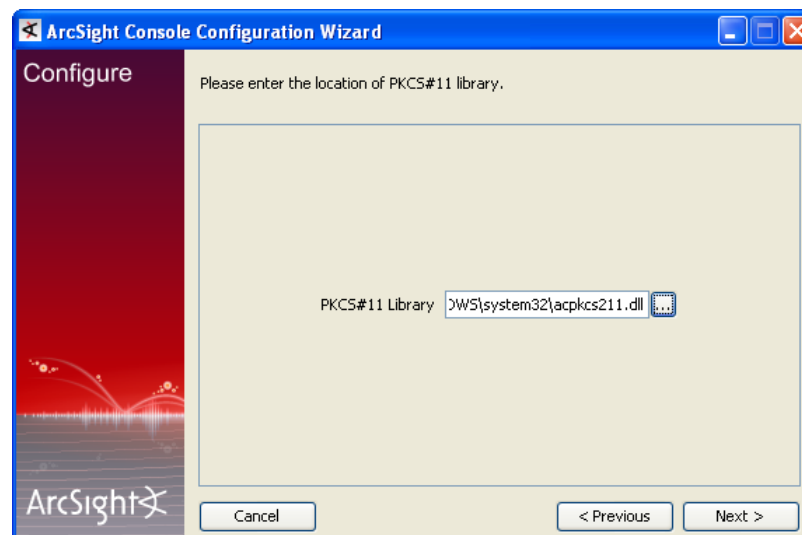


- 5 Follow the prompts in the next few screens by accepting the defaults.

- 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:



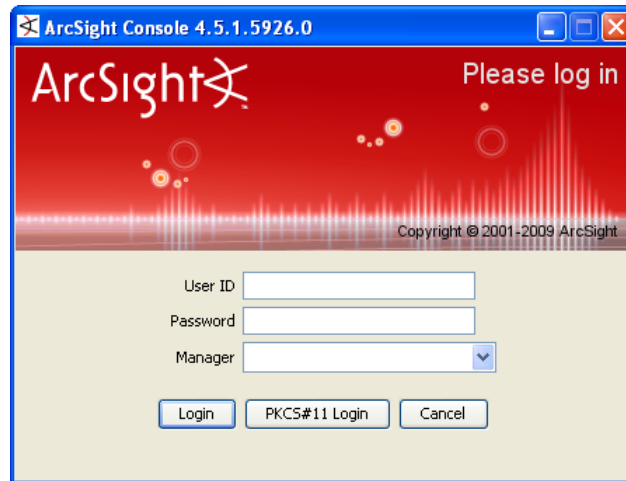
By default, the PKCS #11 library is located in:

[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.



Using CAC with ArcSight Web

Make sure that you have set the `cac.pkcs11.lib` property in the Web's `<ARCSIGHT_HOME>\config\webserver.properties` file as explained in the section, "PKCS#11 Token Support in ESM" on page 218. To use the Common Access Card with ArcSight Web, do the following:

- 1 Install the CAC provider's software on the system on which you have installed ArcSight Web.
- 2 Export the CAC's certificate. See "Export the CAC's Certificate" on page 220 for details. Make sure that this certificate is available on the system on which you have installed ArcSight Web.
- 3 Extract the CA's root certificate from the CAC certificate. See "Extract the Root CA Certificate From the CAC Certificate you Exported" on page 222 for details.
- 4 Import the CAC Card Signer's Root Certificate into the Web's webnssdb

To import the certificate into the Web's `webnssdb`:

- a** Disable FIPS mode in the Web's `webnssdb` by running the following from the Web's `\bin` directory:

```
arcsight runmodutil -fips false -dbdir
<ARCSIGHT_HOME>\config\jetty\webnssdb
```

- b** Import the CAC card signer's root certificate by running the following command:

```
arcsight runcertutil -A -n CACcert -t "CT,C,C" -d
<ARCSIGHT_HOME>\config\jetty\webnssdb -i
<absolute_path_to_the_root_certificate>
```



For the `-t` option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- c** Enable FIPS mode in the Manager's `nssdb` by running:

```
arcsight runmodutil -fips true -dbdir
<ARCSIGHT_HOME>\config\jetty\webnssdb
```

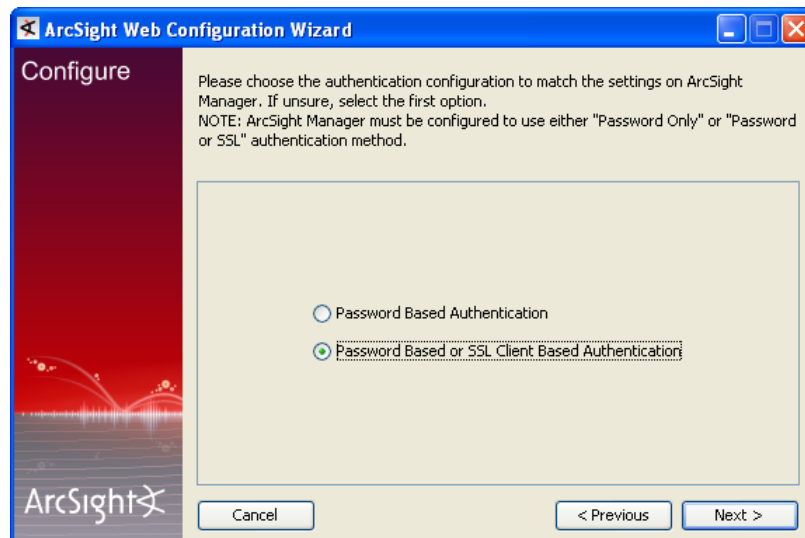
5 Set the Authentication Option in ArcSight Web

Set the Web's authentication to **Password Based or SSL Client Based Authentication**. To do so,

- a** Run the setup program for the Web's `\bin` directory:

```
arcsight webserversetup
```

- b** Select **Password Based or SSL Client Based Authentication** in the following screen.



- c** Complete the setup by following the prompts in the next few screens.
- d** Start ArcSight Web by entering the following from ArcSight Web's `\bin` directory:

```
arcsight webserver
```

- e Make sure to set your browser to use TLS. Follow the instructions in [“Configuring Firefox 3.x to Make it FIPS 140-2 Compliant” on page 203](#) if you plan to use Firefox.



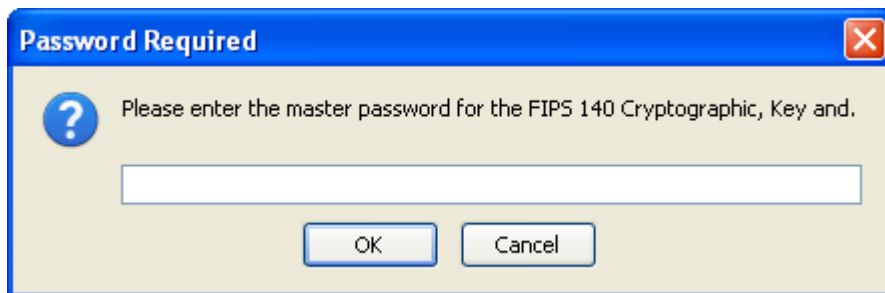
Make sure to Disable FIPS in Firefox. Firefox has a built in truststore and so does the CAC card. If you enable FIPS on Firefox, its own truststore will conflict with the truststore on the CAC card. This will result in an error message and you will not be able to connect to ArcSight Web.

If you plan to use Internet Explorer, follow the instructions in [“Configuring Internet Explorer to Make it FIPS 140-2 Compliant” on page 206](#).

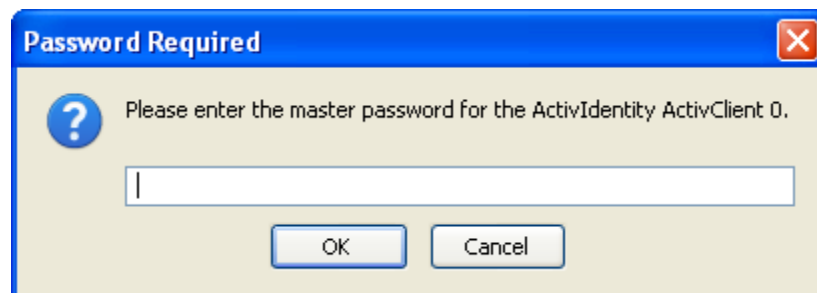
Connecting to ArcSight Web Using CAC

Use a web browser such as Firefox or Internet Explorer to connect to ArcSight Web.

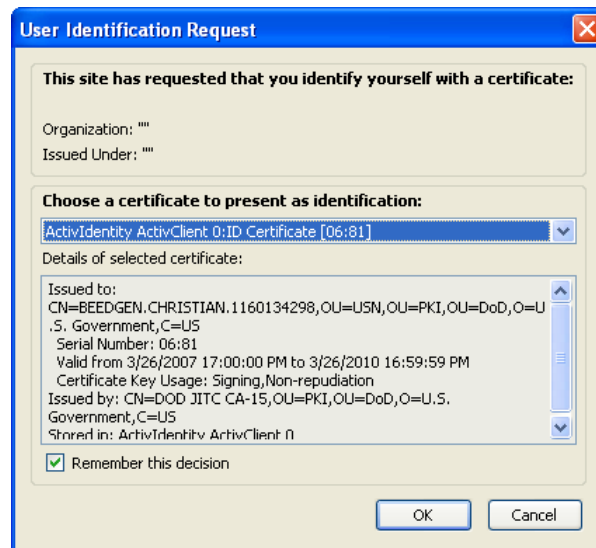
- 1 Make sure that the CAC card is securely placed in its card reader.
- 2 Go to URL <https://<hostname>:9443/>.
- 3 You will be requested to enter your FIPS cryptographic password. Enter the password that you have set for your `webnssdb` in this panel.



- 4 You will then be asked to enter the ActivClient password. Enter the password for your CAC card in this panel.



If using Firefox, you will see the following dialog. Click **OK**.



Index

A

- ACE/Server
 - configuring to allow RADIUS requests 161
 - establishing user accounts 162
 - installing and installing as service 161
 - migrating from internal authentication 163
- Active Directory
 - setting up authentication for 89
- Administrator account
 - Manager 94
- Administrator user 17, 69, 94
- appendix
 - example of 151, 155, 167, 171, 175, 217
- ARCHIVE Volume 29
- archiving
 - uncompressed files 155
- Archiving uncompressed files
 - examples 155
- ArcSight
 - built-in security 15
 - components 1
 - Console 3
 - Database 3
 - ESM 1
 - Manager 3
 - SmartConnector 2
 - Web 4
- ArcSight Console
 - client authentication 120
 - connecting to the Manager 117
 - installing 109, 111
 - reconfiguring 126
 - reconnecting to Manager 126
 - starting 124
 - uninstalling 127
 - user logs and preferences 122
 - web browser configuration 121
- ArcSight Database
 - installation files 39
 - preparing your platform 31
 - reconfiguring 61
 - restarting 61
 - selecting a template 30
 - success factors for installation 23
 - uninstalling 71
- ArcSight ESM
 - overview 1
 - planning 9
 - prerequisites 130
 - what is 1
- ArcSight Manager
 - asset auto creation 100
 - configuring for RADIUS authentication 162
 - failover 167
 - high availability 167
 - installation files 75
 - installing 74
 - Java Heap Memory Size 79
 - reconfiguring 104
 - securing properties file 104
 - select packages 94
 - setting up Administrator account 94
 - setting up as service or daemon 100
 - setting up mail server 96
 - SSL certification selection 80
 - starting and stopping 103
 - supported platforms 73, 129
 - transferring configuration 76, 116
 - uninstalling 106
 - verifying installation 103
- ArcSight schema
 - initializing with existing ArcSight instance 152
- ArcSight SmartConnectors 143
 - deployment considerations 143
 - installing 143
- ArcSight Web 14, 73, 129, 130
 - connecting 141
 - installing 131
 - starting manually 140
 - styling 141
 - supported platforms 73, 129
 - uninstalling 141
- asset categories 148
- Assets
 - defining 145
- authentication 84
 - Active Directory 89
 - external 84
 - LDAP 91
 - RADIUS 87

C

- client authentication
 - ArcSight Console 120
- configuring
 - ACE/Server to allow RADIUS requests 161
 - existing Oracle installation 151
 - Manager for iDefense 165
 - partition 64
 - partition management 61
 - SSL 90
 - web browser in Console 121

- connecting
 - ArcSight Console to Manager 117
 - to ArcSight Web 141
 - to database 83
- Console 3
 - installing 111
 - supported platforms 109
- control files
 - Oracle 30
- creating
 - ArcSight instance with existing Oracle 151
 - Customers 149
 - Users 149
- custom authentication scheme 92
- Customers
 - creating 149

D

- Data Monitors
 - tuning 150
- database 3
 - determining the size of 9
 - event volume 9
 - parameters 83
 - ports 13
 - protecting 14
 - selecting a template 30
- Database connection 83
- database installation
 - supported platforms 24
- database upgrade
 - supported platforms 24
- DATABASE Volume 26
- defining
 - Asset Categories 148
 - Assets 145
 - Zones 145
- deleting
 - partition archiver service 70
- deployment
 - ESM 8
- deployment scenarios
 - ESM 18
 - hierarchical deployment 20
 - high availability 18
 - simple, monolithic 18
 - test environment 20
- directory structure
 - ArcSight Installation 11

E

- ESM 1
 - communication overview 6
 - deployment order 8
 - deployment overview 6
 - deployment scenarios 18
 - securing 12
 - supported platforms 8
- establishing
 - user accounts in ACE/Server 162
- event volume 9
- events
 - as SNMP traps 104

- retention policy 10
- external authentication
 - guidelines 85
 - how it works 84

F

- failover
 - ArcSight Manager 167
 - Manager architecture for high availability 167
 - monitoring processes 169
 - script to start/stop Manager 169

G

- guidelines
 - external authentication 85
 - security 17

H

- hardware
 - security 15
- hierarchical deployment 20
- high availability
 - scenario 18

I

- iDefense database
 - configuring Manager for 165
 - integrating with 165
- initializing
 - ArcSight schema with existing ArcSight instance 152
 - resources 50
 - schema 50
 - tablespace 50
- Installation
 - directory structure 11
- installing
 - ACE/Server and ACE/Server as service 161
 - ArcSight Console 111
 - ArcSight Database and Oracle 38
 - ArcSight Database software 39
 - ArcSight Manager 74
 - ArcSight SmartConnectors 143
 - ArcSight Web 131
 - Oracle 10g 42
 - Oracle without ArcSight Database installer 152
- installing Oracle
 - general guidelines 24
- integrating
 - with iDefense database 165

L

- LDAP
 - setting up authentication for 91

M

- mail server 96
 - parameters 98
- Manager 3
 - determining the topology 9

- ports 13
- protecting 12
- migrating
 - from internal authentication to ACE/Server 163
- monitoring processes
 - in high availability environment 169

O

- operating system
 - security 16
- Oracle
 - configuring an existing installation 151
 - control files 30
 - creating a new 10g instance 45
 - guidelines for installing 24
 - installing without ArcSight Database installer 152
 - storage guidelines 25
- Oracle 10g
 - installing 42
- overview
 - ESM 1
 - ESM communication 6
 - ESM deployment 6

P

- parameters
 - database 83
- partition
 - changing configurations 68
 - configuration parameters 64
- partition archiver
 - changing password 71
 - registering with Manager 70
 - setting up 68
 - starting and stopping 69
- partition archiver service
 - deleting 70
 - reinstalling 70
- partition management
 - configuring 61
- planning
 - ESM installation 8
- preferences
 - ArcSight Console 122
- protecting
 - ArcSight Database 14

R

- RADIUS
 - setting up authentication for 87
- RADIUS authentication
 - configuring Manager for 162
 - defining shorter internal login names 159
 - passcodes 159
 - setting up 159
 - setting up ACE/Server 161
 - two-factor challenge responses 160
- reconfiguring
 - ArcSight Console 126
 - ArcSight Database 61
- reconnecting
 - Console to Manager 126

- REDO Volume 28
- Resources
 - establishing 145
 - initializing 50
- restarting
 - ArcSight Database 61
- retention policy 10
- Rules
 - tuning 150
- running
 - Manager as a Windows service 103

S

- schema
 - initializing 50
- security 15
 - guidelines and policies 17
 - hardware 15
 - operating system 16
- setting
 - ACE/Server RADIUS authentication 161
 - RADIUS authentication 159
- size
 - database 9
 - Java Heap Memory 79
 - topology of Managers 9
- SmartConnectors 2
- SNMP field types
 - mapping to ArcSight field types 106
- SNMP traps
 - configure 104
- SSL
 - configuring 90
- SSL certificate
 - selecting 80
- starting
 - ArcSight Console 124
 - ArcSight Manager 103
 - ArcSight Web manually 140
 - partition archiver 69
- stopping
 - ArcSight Manager 103
 - manually started Manager 103
 - partition archiver 69
- supported platforms
 - ArcSight Web 73, 129
 - Console 109
 - database installation and upgrade 24
 - ESM 8
 - Manager 73, 129
- SYSTEM Volume 26

T

- tablespace
 - initializing 50
- test environment
 - example 20
- topology
 - Managers 9
- troubleshooting
 - communication between ACE/Server and Manager 163
- tuning

- data monitors 150
- rules 150

U

- UNCOMPRESSED Archive types 155
- uncompressed files
 - archiving 155
 - examples of archiving 155
- uninstalling
 - ArcSight Console 127
 - ArcSight Database 71
 - ArcSight Web 141
- upgrading
 - ArcSight Database and Oracle 38
- user logs
 - ArcSight Console 122
- Users
 - creating 149
- using

- UNCOMPRESSED Archive types 155

V

- volume
 - ARCHIVE 29
 - DATABASE 26
 - REDO 28
 - SYSTEM 26

W

- Web 4
- Web browser
 - configuring in Console 121

Z

- Zone
 - defining 145