

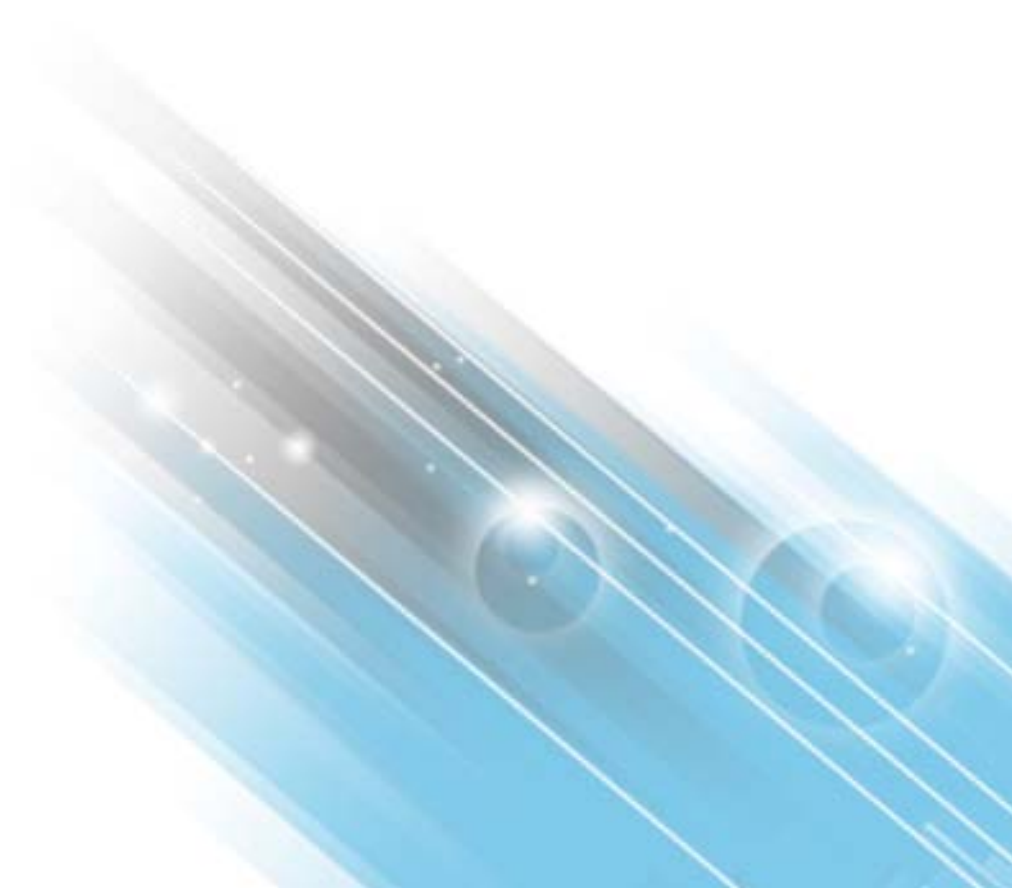


# HP ArcSight ESM

Software Version: 5.6

## Installation Guide

September 10, 2015



Copyright © 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

#### Contact Information

<b>Phone</b>	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="http://softwaresupport.hp.com">http://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.hp.com">https://protect724.hp.com</a>

#### Revision History

Date	Product Version	Description
09/10/2015	5.6	Updated for ESM 5.6 release.

# Contents

---

<b>Chapter 1: Planning and Installation Overview .....</b>	<b>11</b>
What is ESM? .....	11
Components .....	11
SmartConnector .....	12
ArcSight Manager .....	13
ArcSight Database .....	13
ArcSight Console .....	13
ArcSight Web .....	14
Deployment Overview .....	16
ESM Communication Overview .....	16
Effect on Communication when Components Fail .....	17
Deployment Order .....	18
Supported Platforms .....	18
Installation Planning .....	18
Inventory your Devices .....	19
Determine the Size and Topology of ArcSight Managers .....	19
Size your Database .....	19
Event Volume .....	19
Retention Policy .....	20
Identify or Procure Hardware and Software .....	20
Choosing Between FIPS Mode or Default Mode .....	20
Differences Between Default and FIPS Modes .....	21
Using PKCS#11 .....	21
Import Control Issues .....	21
Directory Structure for ESM Installation .....	22
Securing Your ESM System .....	22
Protecting ArcSight Manager .....	22
Protecting ArcSight Database .....	24
ArcSight Built-In Security .....	25
Physical Security for the Hardware .....	26
Operating System Security .....	27
General Guidelines and Policies about Security .....	27
Deployment Scenarios .....	28
Scenario 1: A simple, monolithic deployment .....	28

Scenario 2: A high availability, transparent failover deployment .....	29
Scenario 3: A hierarchical deployment .....	30
Scenario 4: A test environment deployment .....	31
Where to go From Here .....	32
<b>Chapter 2: Installing ArcSight Database .....</b>	<b>33</b>
Key Database Installation Success Factors .....	33
Supported Platforms for Database Installation .....	33
General Guidelines for Installing Oracle .....	34
Storage Guidelines .....	34
Disk Space Requirements .....	34
Volume 1: SYSTEM Volume .....	36
Volume 2: DATABASE Volume .....	37
Volume 3: REDO Volume .....	39
Volume 4: ARCHIVE Volume .....	39
Oracle Control Files .....	40
Selecting an ArcSight Database Template .....	41
Preparing your Platform for Database Installation .....	42
Preparing a Linux System .....	42
Preparing a Windows System .....	44
Installing ArcSight Database .....	45
Installing the ArcSight Database Software .....	45
Installing Oracle 11g Database Software .....	48
Configuring Shared Memory on Linux .....	50
Creating a New Oracle 11g Instance .....	52
Avoiding DB Write Performance Issues with Oracle 11g .....	58
Initializing ESM Tablespaces, Schema, and Resources .....	59
Restarting or Reconfiguring ArcSight Database .....	71
Configuring Partition Management .....	71
Overview .....	72
Partition Configuration Parameters .....	75
Changing Partition Management Configurations .....	77
Setting Up Partition Archiver .....	77
Starting and Stopping Partition Archiver .....	79
Re-registering Partition Archiver with ArcSight Manager .....	79
Deleting the Partition Archiver Service .....	79
Reinstalling the Partition Archiver Service .....	80
Changing the Password for Partition Archiver .....	80
Uninstalling the ArcSight Database Software .....	80
<b>Chapter 3: Installing ArcSight Manager .....</b>	<b>81</b>
Manager Supported Platforms .....	82
Installing the Manager .....	82

---

Transferring Configuration from an Existing Installation .....	84
Selecting the Mode in which to Configure Manager .....	85
Configuring the Manager's Host Name, Port, and Location .....	86
Java Heap Memory Size .....	87
SSL Certification Selection .....	88
Deciding which SSL Certificate to Select .....	88
Selecting the SSL certificate .....	89
Database Connection .....	91
Authentication .....	92
How external authentication works .....	92
Guidelines for setting up external authentication .....	92
Password Based Authentication .....	93
Password Based and SSL Client Based Authentication .....	100
Password Based or SSL Client Based Authentication .....	100
SSL Client Only Authentication .....	101
Manager Administrator Account Setup .....	101
Select Packages .....	102
Mail Server .....	103
ArcSight Web .....	106
Asset Auto Creation .....	107
Setting up as a Service or Daemon .....	107
Starting and Stopping the Manager .....	108
Starting the Manager .....	108
Stopping the Manually Started Manager .....	109
Running the Manager as a Service .....	109
Verifying the Manager Installation .....	110
Reconfiguring Manager .....	110
Securing the Manager Properties File .....	110
Sending Events as SNMP Traps .....	111
Uninstalling Manager .....	113
<b>Chapter 4: Installing ArcSight Console .....</b>	<b>115</b>
Console Supported Platforms .....	115
Using a PKCS#11 Token .....	115
Installing the Console .....	116
Character Set Encoding .....	118
Transferring Configuration from an Existing Installation .....	118
Selecting the Mode in which to Configure ArcSight Console .....	119
Manager Connection .....	119
Authentication .....	121
Web Browser .....	122
Starting the ArcSight Console .....	125
Logging into the Console .....	127

Reconnecting to the ArcSight Manager .....	127
Reconfiguring the ArcSight Console .....	127
Turn Off Database Recycle Bin .....	128
Uninstalling the ArcSight Console .....	128
<b>Chapter 5: Installing ArcSight Web .....</b>	<b>129</b>
ArcSight Web Supported Platforms .....	129
Web Browsers .....	129
Using a PKCS#11 Token .....	130
Installing ArcSight Web .....	130
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
ArcSight Manager Host Name and Port .....	135
Trust Manager Certificate .....	136
Select Type of Key Pair .....	136
Authentication .....	138
Setting ArcSight Web as a Service or Daemon .....	138
Starting ArcSight Web Manually .....	139
Connecting to ArcSight Web .....	139
Styling ArcSight Web .....	140
Uninstalling ArcSight Web .....	140
<b>Chapter 6: Installing ArcSight SmartConnectors .....</b>	<b>141</b>
Deployment Considerations .....	141
Installing SmartConnectors .....	141
<b>Chapter 7: Establishing Initial ArcSight Resources .....</b>	<b>143</b>
Defining Zones and Assets .....	143
Defining Asset Categories .....	146
Creating Customers and Users .....	147
Tuning Data Monitors and Rules .....	147
<b>Appendix A: Using UNCOMPRESSED Archive Type .....</b>	<b>149</b>
Archiving Uncompressed Files .....	149
Examples .....	150
<b>Appendix B: Setting up RADIUS User Authentication .....</b>	<b>153</b>
Passcodes .....	153
Defining Shorter ESM Internal Login User Names .....	153
Two-Factor Challenge Responses .....	154

---

Steps for Setting Up ACE/Server RADIUS Authentication .....	155
Installing the ACE/Server and ACE/Server RADIUS Service .....	155
Configuring the ACE/Server to allow RADIUS Requests .....	155
Enabling User Accounts in ACE/Server .....	156
Configuring ArcSight Manager .....	156
Migrating from Internal Authentication to ACE/Server .....	157
Authentication Troubleshooting .....	157
<b>Appendix C: Integrating with iDefense Database .....</b>	<b>159</b>
Configuring Manager for iDefense .....	159
<b>Appendix D: ArcSight Manager Failover .....</b>	<b>161</b>
Architecture .....	161
Starting Processes .....	164
Monitoring Processes .....	164
Next Steps .....	165
<b>Appendix E: FIPS Compliant State Auditing .....</b>	<b>167</b>
Compliance State Auditing with Active Channels .....	167
Compliance State Auditing with Dashboards .....	168
Compliance State Auditing with Reports .....	168
Compliance State Auditing with Rules .....	169
<b>Appendix F: Installing ESM in FIPS Mode .....</b>	<b>171</b>
What is FIPS? .....	172
Network Security Services Database (NSS DB) .....	172
What is Suite B? .....	173
NSS Tools Used to Configure Components in FIPS Mode .....	173
TLS Configuration in a Nutshell .....	174
Understanding Server Side Authentication .....	174
Understanding Client Side Authentication .....	175
Setting Up Authentication on ArcSight Web - A Special Case .....	175
Using PKCS #11 Token With a FIPS Mode Setup .....	176
Installing ArcSight Database .....	177
Installing the ArcSight Manager in FIPS mode .....	177
Setting up Partition Archiver in FIPS Mode .....	183
Installing ArcSight Console in FIPS Mode .....	184
Connecting a Default Mode ArcSight Console to a FIPS 140-2 ArcSight Manager .....	190
Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers .....	190
Installing ArcSight Web in FIPS Mode .....	190
Configure Your Browser for FIPS .....	197
Installing SmartConnectors in FIPS mode .....	197
How do I Know if My Installation is FIPS Enabled? .....	198

Partition Archiver .....	198
<b>Appendix G: Installing ESM in FIPS with Suite B Mode .....</b>	<b>201</b>
What is Suite B? .....	201
Installing ArcSight Database .....	202
Installing ArcSight Manager in FIPS with Suite B Mode .....	202
Setting up Partition Archiver in FIPS with Suite B .....	208
Installing ArcSight Console in FIPS with Suite B Mode .....	208
Installing ArcSight Web in FIPS with Suite B Mode .....	208
Installing SmartConnectors in FIPS with Suite B Mode .....	214
<b>Appendix H: Using the PKCS#11 Token .....</b>	<b>215</b>
What is PKCS? .....	215
PKCS#11 .....	215
PKCS#12 .....	216
PKCS#11 Token Support in ESM .....	216
Setting Up to Use a CAC Card .....	216
Install the CAC Provider's Software .....	216
Map a User's External ID to the CAC's Subject CN .....	216
Obtain the CAC's Issuers' Certificate .....	218
Extract the Root CA Certificate From the CAC Certificate .....	220
Import the CAC Root CA Certificate into the ArcSight Manager .....	221
FIPS Mode - Import into the ArcSight Manager's nssdb .....	221
Default Mode - Import into ArcSight Manager's Truststore .....	221
Select Authentication Option in managersetup .....	222
Select Authentication Option in ArcSight Console Setup .....	223
Logging in to the ArcSight Console Using CAC .....	225
Using CAC with ArcSight Web .....	225
Logging in to ArcSight Web Using CAC .....	227
<b>Appendix I: About ESM Locales and Encodings .....</b>	<b>229</b>
Terminology .....	229
Internationalization .....	229
Locale .....	229
Character Set .....	229
Code Set .....	229
Code Point .....	230
Encoding .....	230
Unicode .....	230
Before you Install a Localized Version of ArcSight ESM .....	230
ArcSight Database .....	231
Selecting an Encoding .....	231
ArcSight Manager .....	232

---

ArcSight Console .....	232
ArcSight SmartConnectors .....	232
Setting the Encoding for Selected SmartConnectors .....	232
Localization of Date Formats in Tokens and Operations .....	233
Key-Value Parsers for Localized Devices .....	233
Examples .....	234
Scenario 1 - Events received in a single language only .....	234
Database .....	234
ArcSight Manager, Console, and Web .....	234
Scenario 2 - Events received in multiple languages .....	234
Database .....	234
ArcSight Manager, Console, and Web .....	235
Preparing to Install the Language Update .....	235
Verifying the Character Set used on your Database .....	235
Installing the Language Update .....	236
List of possible values for the agent.parser.locale.name property .....	236



# Chapter 1

## Planning and Installation Overview

---

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



If you already have ESM 5.5 installed and are planning to move to ESM with CORR Engine, we suggest that you migrate from 5.5 and skip this installation of ESM 5.6.

The following topics are covered in this chapter:

["What is ESM?" on page 11](#)  
["Components" on page 11](#)  
["Deployment Overview" on page 16](#)  
["ESM Communication Overview" on page 16](#)  
["Deployment Order" on page 18](#)  
["Supported Platforms" on page 18](#)  
["Installation Planning" on page 18](#)  
["Directory Structure for ESM Installation" on page 22](#)  
["Securing Your ESM System" on page 22](#)  
["Deployment Scenarios" on page 28](#)  
["Where to go From Here" on page 32](#)

## What is ESM?

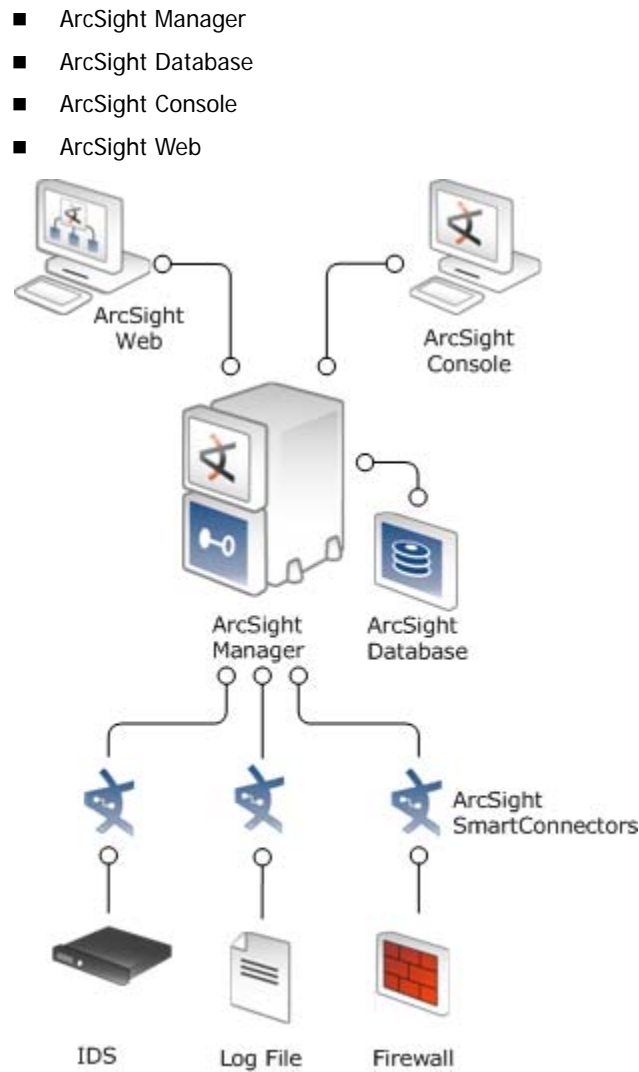
ESM is a Security Information Management (SIM) solution that collects and analyzes security data from heterogeneous devices on your network and provides you a central, real-time view of the security status of all devices of interest to you.

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.

## Components

The ESM system contains the following components, as shown in the following illustration:

- SmartConnector



**Figure 1-1** ESM Components

## 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, 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.

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

SmartConnectors are available for over 200 network device types found in a typical enterprise infrastructure. For a complete list of available SmartConnectors, see the HP SSO website.

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 ESM solution. The ArcSight 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 ArcSight Manager are processed, see ESM 101.

ArcSight Manager can be installed across a variety of operating systems, such as Windows and Linux, 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 ArcSight Manager such as users, groups, permissions, rules, assets, and reports.

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

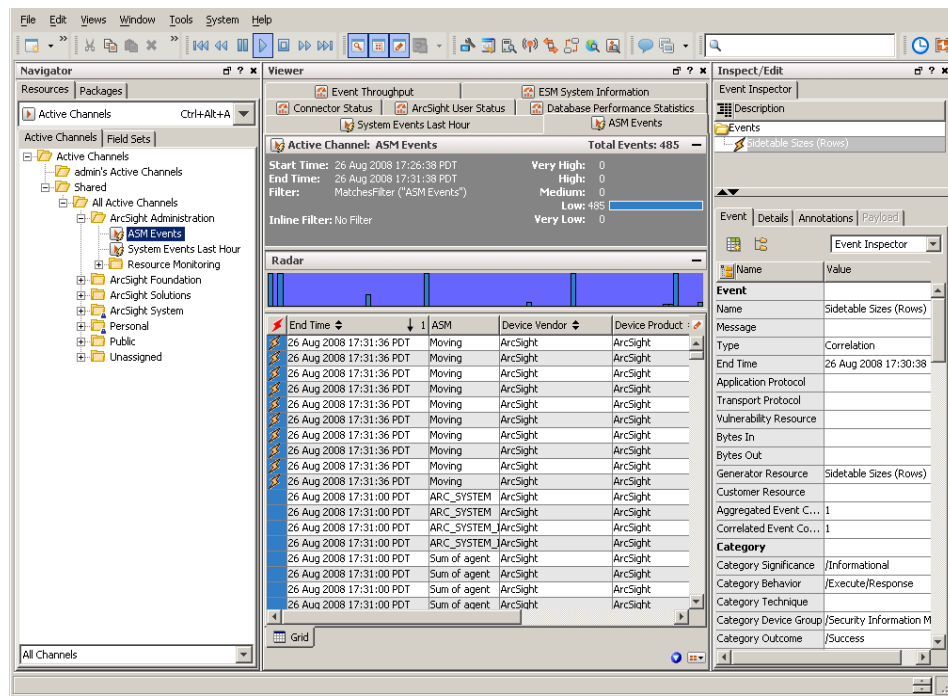
The ArcSight Database can be installed across a variety of operating systems and hardware platforms. The platform on which the database is installed can be different from the one on which the ArcSight Manager is running.

## ArcSight Console

The ArcSight Console is a workstation-based graphical user interface that enables you to perform essential security management tasks. Depending on your job function, you can use the ArcSight Console 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.

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



**Figure 1-2** Example of ArcSight Console

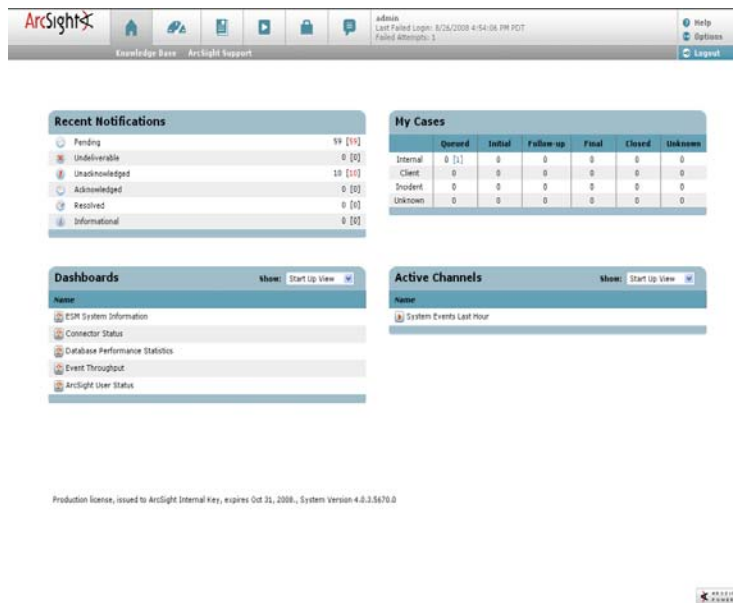
## ArcSight Web

ArcSight Web is a web server that enables you to access the Manager securely using a browser. It is intended for viewing information from 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 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.



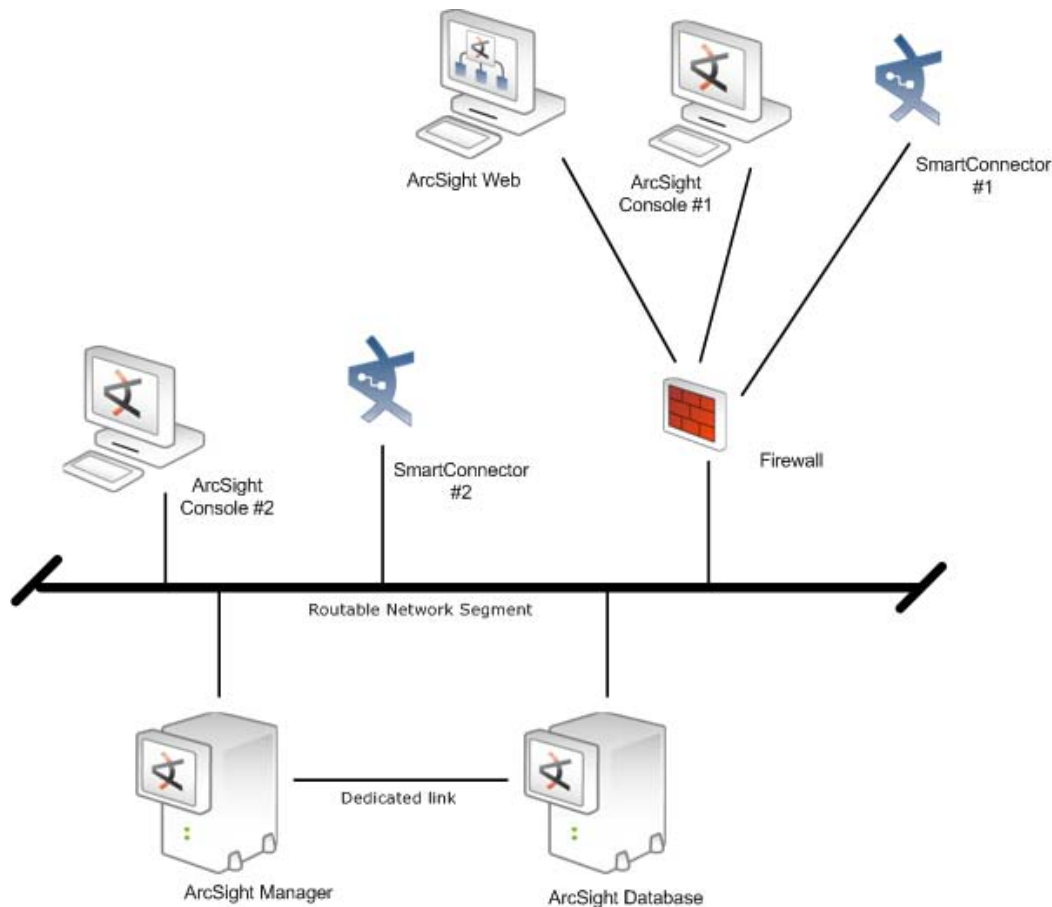
**Figure 1-3** Example of ArcSight Web

## Deployment Overview



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

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



**Figure 1-4** ESM Components Deployment Overview

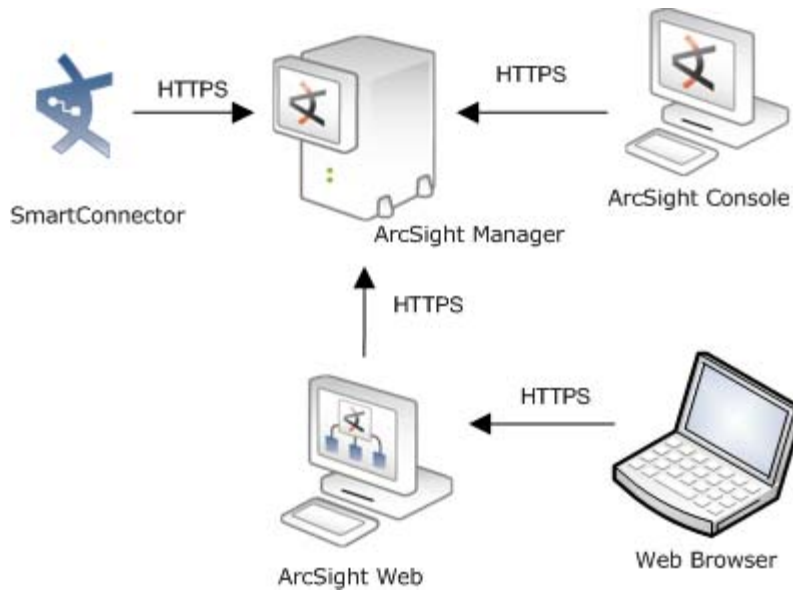
There are other possible topologies such as placing the Manager and the database behind a firewall for an extra layer of protection or installing multiple Managers for redundancy.

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

## ESM Communication Overview

ArcSight Console, Manager, and the 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** 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 ESM System” on page 22](#).

The ArcSight Manager never makes outgoing connections to the ArcSight 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 ArcSight Manager and the ArcSight 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 (it’s full or the hardware is down), the ArcSight Manager stops accepting events and caches any that were not committed to the database. The SmartConnectors start caching new events, so there is no event data loss. The ArcSight Consoles are disconnected. ArcSight Web connections are disconnected and no new login requests are accepted until the database is up and running again.

If the ArcSight 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 ArcSight Consoles are disconnected. ArcSight Web connections are disconnected and no new login requests are accepted.

If a SmartConnector fails, whether event data loss occurs depends on the SmartConnector type. SmartConnectors that listen for events from devices such as the SNMP SmartConnectors 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 ArcSight Database
- 2 ArcSight Manager
- 3 SmartConnectors or Consoles or Partition Manager (in any order)
- 4 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 *HP ArcSight ESM Support Matrix* document available on the Protect 724 website for the most current information on supported platforms. (<https://protect724.hp.com/community/arcSight/productdocs/es>)

---

All ESM system components are software based. You can deploy these components on industry standard heterogeneous platforms, such as 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, we 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 Adobe.

## 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 ESM to monitor. Typically, device type is directly related to the number of events it generated daily. For example, firewalls generate a lot of events and a server may not. Once you have determined the expected event volume on your network, you can easily size the hardware needed 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.



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

## Inventory your Devices

Inventory your devices and plan the SmartConnector that reports 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 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 ArcSight Managers

Determine the number and configuration of ArcSight Managers to which the SmartConnectors report. If you use more than one ArcSight 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.



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 is 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 are uncompressed.

The retention period for compressed partitions specifies the number of days (or partitions) for which data is 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 are 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 are 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

ESM supports the Federal Information Processing Standard (FIPS) 140-2 and Suite B. FIPS 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.

Depending on your requirements, you can choose to install the ESM components in either of these modes:

- Default mode  
To install ESM in default mode, follow the instructions in the respective chapters for installing the components.
- FIPS 140-2 mode

To install ESM in FIPS mode, follow the instructions in [Appendix F, Installing ESM in FIPS Mode, on page 171](#).

■ FIPS with Suite B mode

To install ESM in FIPS with Suite B mode, follow the instructions in [Appendix G, Installing ESM in FIPS with Suite B Mode, on page 201](#).

## Differences Between Default and FIPS Modes

The following table outlines some of the basic differences between the three modes that ESM supports:

Mode	Use of SSL/TLS	Default Cipher Suites	Keystore/Truststore
Default Mode	SSL or TLS	<ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> <li>More...</li> </ul>	Keypair and Certificates stored in Keystore and Truststore in JKS format
FIPS 140-2 Mode	TLS	<ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul>	Keypair and Certificates stored in NSSDB
FIPS with Suite B Mode	TLS	<ul style="list-style-type: none"> <li>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</li> </ul> <p>Suite B 128 bits security level, providing protection from unclassified up to secret information</p> <ul style="list-style-type: none"> <li>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA</li> </ul> <p>Suite B 192 bits security level, providing protection from unclassified to top secret information</p>	Keypair and Certificates stored in NSSDB

## Using PKCS#11

Starting in ESM v4.0 SP2, ESM supports the use of a PKCS#11 token such as the Common Access Card (CAC) to log into the ArcSight 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 ESM 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
```

Rename \*.jar.original to \*.jar.

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

## Directory Structure for ESM Installation

ESM software components install consistently across Linux and Windows platforms. Whether a host is dedicated to the ArcSight Database, ArcSight Manager, ArcSight 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  
/home/<userdirectory>/arcsight/manager on a Linux 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
ESM Software	<ARCSIGHT_HOME>\bin
Properties files	<ARCSIGHT_HOME>\config
Log files	<ARCSIGHT_HOME>\logs

## Securing Your ESM System

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



By default, the minimum length for passwords is six characters and the maximum length is 20 characters. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration," "password Character Sets."

---

## 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 ArcSight 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 (Linux 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 (Linux 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
```

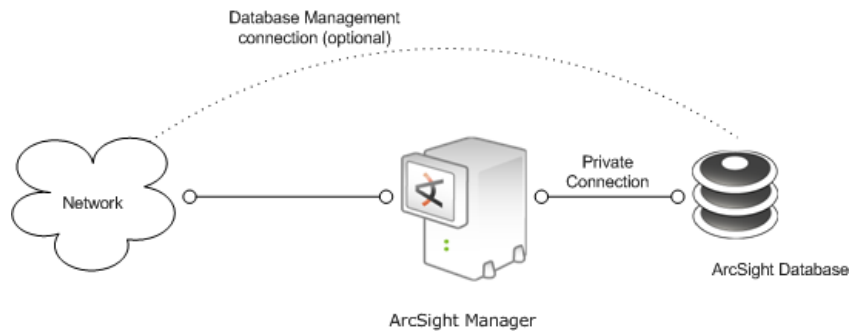
```
agents.accept.ips=10.*.*.*,192.168.0.0/255.255.0.0
```

## Protecting ArcSight Database

Secure the link between the ArcSight Manager and Oracle. The options described here include a private network (preferred) or a tunnel (if performance is less important).

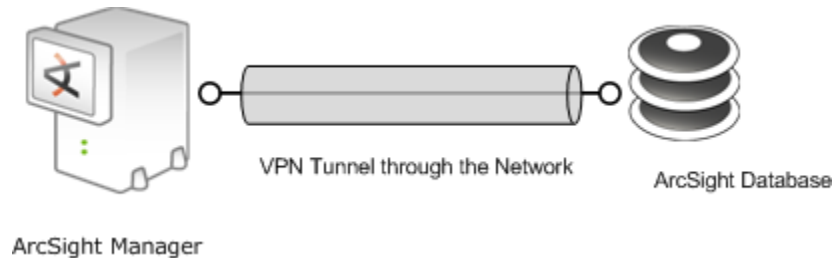
You can secure the communication path between ArcSight Database and ArcSight Manager in these ways:

- Dedicated (private) connection between the ArcSight Manager and the ArcSight Database



Run a dedicated network between ArcSight Manager and ArcSight Database. Use a second network interface for the ArcSight 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. We recommend 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

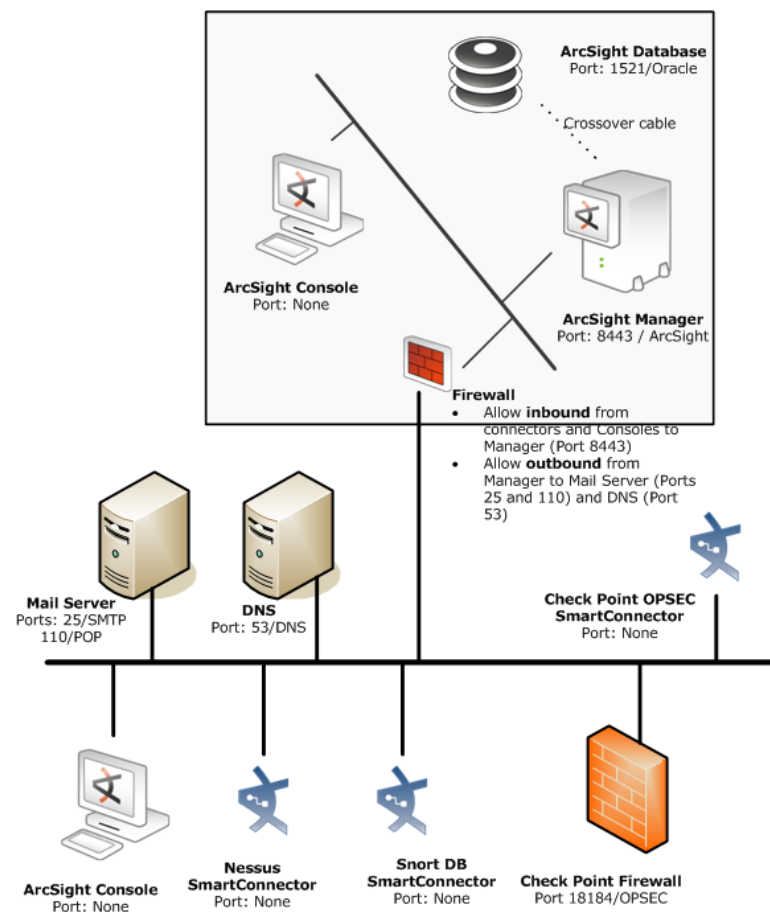
HP ArcSight user accounts have user types that control the functions which users can access in the ArcSight Manager. The "Normal User" type has the most privileges. Where possible, use more restrictive types, such as "Manager SmartConnector," "Management Tool," or "Archive Utility" for non-human user 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 ESM 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 ESM system. Physical hardware includes computers running ArcSight Console, ArcSight Manager, ArcSight 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 ESM components.



**Figure 1-6** Physical security for hardware

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):
  - ◆ 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 need. 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).
- 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 Linux machines, disallow remote root logins (for OpenSSH, using the `PermitRootLogin no` directive in `/etc/ssh/sshd_config`). This forces 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 ESM in some way, they won't be able to log in as root. (See ["About the ArcSight User" on page 83.](#))
- 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 HP will ever request a user's password. When HP 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 HP team to work effectively.

Educate users to use secure means of communication—such as SSL to upload to an HP web site or PGP for e-mail—when transferring configuration information or log files to HP.

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 the Customer Support using the HP SSO site 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). For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration."

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 ArcSight Manager
- The *oracle* user and *root* user on the system that runs the ArcSight Database
- All users created in ESM
- 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
- The Active Directory domain user password for ArcSight Manager 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 ESM 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

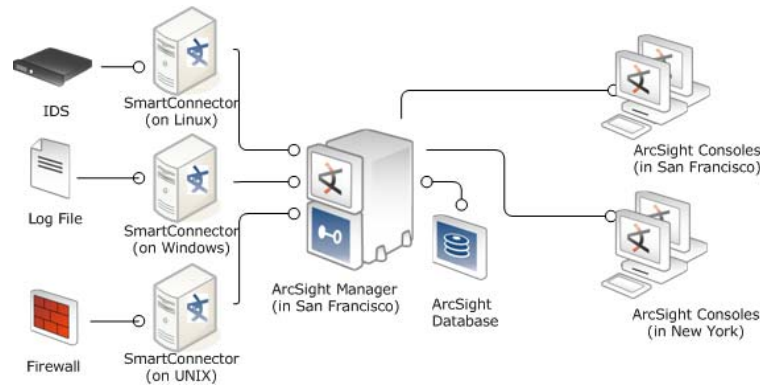
You can deploy ESM in a number of ways depending on your business needs and budget. The following are a few recommended scenarios.

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

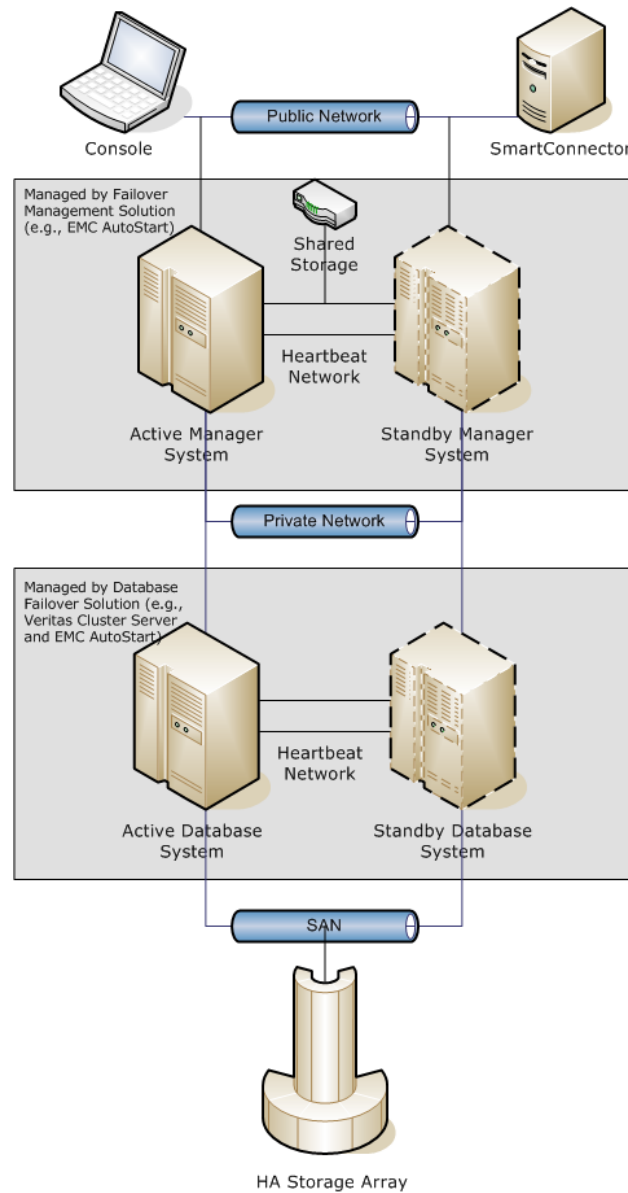
## Scenario 2: A high availability, transparent failover deployment

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 ArcSight 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 ArcSight 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 ArcSight

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.

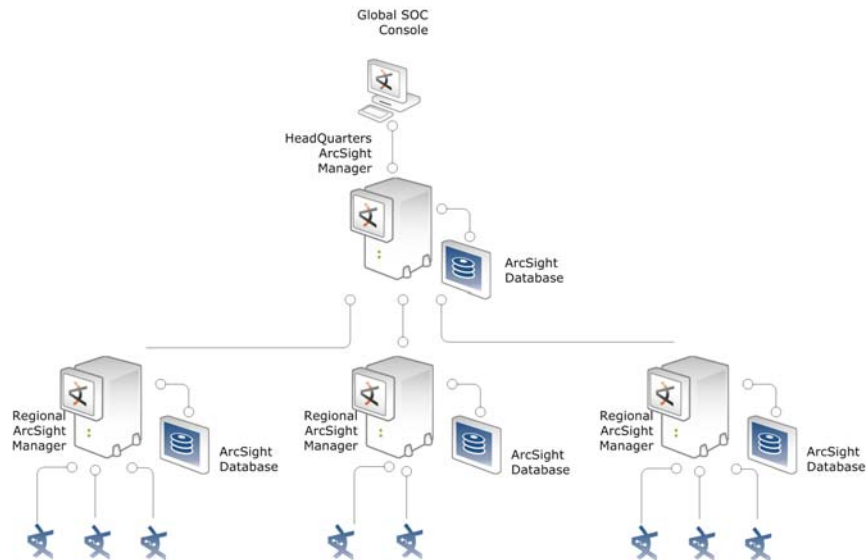


**Figure 1-8** A High Availability, Transparent Failover Deployment

## Scenario 3: A hierarchical deployment

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

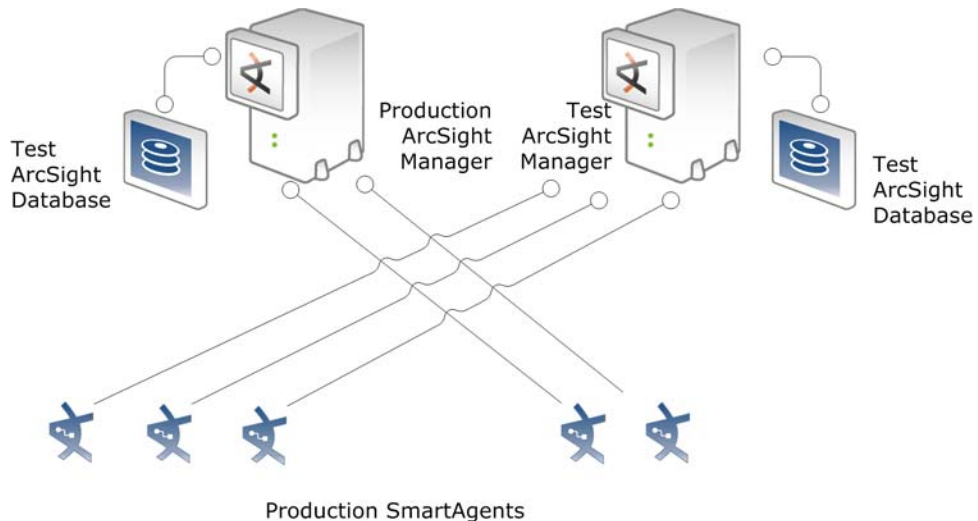
The lower-level managers collect and process events from their local SmartConnectors. In addition, these Managers forward key events to the central Manager thus enabling the central Manager to provide a holistic view of the security status of the entire network.



**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 ArcSight Manager before implementing them in your production environment.



**Figure 1-10** A Test Environment Deployment

## Where to go From Here

Here are the steps to install and configure ESM:

**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 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 SmartConnectors, which you do in the next and final installation step.

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

**ArcSight Web Installation.** ArcSight Web is a standalone web server that interacts with the ArcSight Manager and can operate outside a firewall that protects the ArcSight Manager. Thus users can use supported browsers to access information from the ArcSight 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 ArcSight Manager.

## Chapter 2

# Installing ArcSight Database

---

The first step in the process of installing ESM 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 33
- “Supported Platforms for Database Installation” on page 33
- “General Guidelines for Installing Oracle” on page 34
- “Preparing your Platform for Database Installation” on page 42
- “Installing ArcSight Database” on page 45
- “Restarting or Reconfiguring ArcSight Database” on page 71
- “Configuring Partition Management” on page 71
- “Uninstalling the ArcSight Database Software” on page 80

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 141](#).

## 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 ESM 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 ESM components. ArcSight Database is only tested and certified using the DBMS configuration described here.

## Supported Platforms for Database Installation

ESM v5.6 supports Oracle 11g. Refer to the Product Lifecycle document available on the Protect 724 website for the most current information on supported platforms. Refer to the *HP ArcSight ESM Support Matrix* document available on the Protect 724 website for the

most current information on supported platforms.

(<https://protect724.hp.com/community/arcsight/productdocs/es>)

ArcSight Database is supported on 64-bit environment only. If you are currently on a 32-bit environment and would like to migrate from a 32-bit environment to 64-bit environment, contact HP ArcSight Customer Support for assistance to do so.

## General Guidelines for Installing Oracle

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

### Storage Guidelines

#### Disk Space Requirements

The following table lists typical disk space requirements for installing Oracle 11g:

Space type	Amount of space required
Temporary Space	\$TEMP or \$TMPDIR (/tmp, by default) on Linux and %TEMP% on Windows must have at least 1 GB available.
Linux Swap Space	(Linux 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.

We recommend 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 ESM tablespaces	Hundreds of GB	High
REDO	Oracle redo log files	10-20 GB	Highest

Volume Name	Contents	Typical Size	I/O Load
ARCHIVE	Archived Oracle redo log files and ESM partition archives (if Partition Archiver is enabled)	Up to hundreds of GB	Low



- 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. We do not recommend using the same shared volume for redo logs and archived redo logs as it can impact performance.

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

## Placing Tablespaces in Separate Partitions

During installation, you specify the size, path to, and number of files for each tablespace. Oracle adds up the total space requirement and checks to see if there is sufficient space to install them.



If there isn't sufficient space to install all tablespaces, the install fails.

However, if you choose to install different tablespaces in different partitions, Oracle cannot create a separate total for the tablespaces in each partition. Therefore, the size check only works if the partitions are mounted at the root directory.

## Data Redundancy

For seamless operation and uptime in case of disk failure, it is highly recommended for each of the volumes described above to have data redundancy. For each volume, a choice needs to be made between the advantages and disadvantages of several levels of redundancy. The following are commonly used RAID levels:

RAID Level	Description	Disk Failure Behavior	Typical Raw to Cooked Rate*
0	Striping across two or more disks.	Single disk failure causes complete data loss.	1:1
1	Mirroring across two disks.	Data only lost if both of the disks fail.	2:1
0+1	Two RAID0 sets are mirrored. Requires four or more disks (increments of two disks).	Up to half the disks can fail until complete data loss occurs.	2:1

RAID Level	Description	Disk Failure Behavior	Typical Raw to Cooked Rate*
1+0	RAID1 mirrors are striped together. Requires four or more disks (increments of two disks).	Up to half the disks can fail until complete data loss occurs. Data loss is mathematically less likely in this configuration and recovery behavior is better than RAID 0+1.	2:1

\* The raw to cooked rate in the table above describes how much usable storage is typically obtained per unit of storage purchased. For example, for a RAID1 (full mirror), two disks provide usable storage equal to the size of one of the disks, therefore the rate is 2:1.

Of the listed levels, only RAID1, RAID0+1 and RAID1+0 provide data redundancy for ESM. In a RAID0, if one of the disks fails, all data is lost.

## RAID Levels

I/O performance involves many factors. The first decision for each volume is the RAID level to use. The commonly used levels are RAID0+1 and RAID1+0.

HP ArcSight strongly recommends RAID1+0 for all volumes. If that is not possible, at least the volumes that carry high I/O loads must use RAID1+0. At a minimum, the DATABASE and REDO volumes must use RAID1+0.

Other than RAID levels, most SAN/NAS and other storage products have many parameters that affect performance. Due to the large variety of products, HP ArcSight cannot recommend values for all these parameters. Please consult the storage vendors for recommendations, based on the above I/O characteristics.

## Volume 1: SYSTEM Volume

### Oracle installation directory

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

Before installing Oracle, ensure that the Oracle installation directory has enough space. On Linux, Oracle's Universal Installer, which is invoked in silent mode by ESM's Database Installer, cannot check available disk space if you use a symbolic link to the installation directory. The initial Oracle installation directory size includes:

Size	For...
2 GB	Oracle 11g installation files
2 GB	ArcSight Database Installer staging space for uncompressed Oracle installation files. The Installer extracts the contents of compressed installation files into the stage subdirectory then deletes 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 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
- UNDOTBS1
- TEMP

ESM 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 ESM's embedded Oracle installer (ArcSight Database installer) has the SYSTEM and SYSAUX tablespaces set to autoextend. These tablespaces grow in the initial few days after installation as the event collection ramps up. They stabilize subsequently in terms of size. However, the size of these tablespaces continues to be a small fraction of the space used by ARC\_EVENT\_DATA tablespace.

---

## 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 with the instance. 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 ESM resources such as system objects. Unless very large active lists or a 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.

Very large active lists (specifically partially-cached), session lists, or many actors require proportionally more space, and also potentially increased I/O bandwidth.

## 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.

Very large active lists (specifically partially-cached), session lists, or many actors could require more I/O bandwidth as a result of factors like cache hit distributions.

## ARC\_EVENT\_DATA

The ESM 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 GB each or add an additional redo log group.

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 ESM partition archives

This volume is required only if Partition Archiver is enabled.

## ArcSight Partition Archives



Although you have the option to archive partitions in an uncompressed form, ArcSight recommends that you do not use the uncompressed archive type for archiving partitions.

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 HP 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 hangs 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 resumes (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 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 depends on the capacity and performance requirements of the ArcSight security management system you deploy.

ArcSight Database templates specify:

- Required minimum memory capacity
- Required minimum disk space
- Number of redo logs
- Redo log file size
- Minimum sizes for ESM 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.

We recommend dedicating a machine to the ArcSight Database. The operating system chosen often suggests a hardware platform.

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 <sup>2</sup>	4 GB	128 GB

Template	CPUs	Memory	Disk
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

**Note**

The figures shown for the templates represent the minimum space required for the base installation and do not include the space required for event storage. Calculate your space requirement for event storage based on the time you have set up for event retention period.

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.

## Preparing your Platform for Database Installation

For this release, ArcSight Database can be installed on 64-bit Windows and 64-bit Linux.

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 prevent the installer from creating the group or owner account, create them manually before launching the installer.

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

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

## Preparing a Linux System

**Caution**

On RHEL, in order to run the installers remotely in GUI mode, install the following libraries and their associated dependencies:

- X libraries
- glibc
- libXext
- libXtst

On 64-bit machines, also install the 32-bit glibc, libXext, and libXtst.

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” on page 33](#).

- 2 Verify that the following required packages (the versions stated below or newer version of the packages) are installed:



32-bit Linux is not supported.

On 64-bit machines, you need both the 32-bit and 64-bit versions of some of these libraries, as indicated, below.

#### On x86 64-bit Linux RHEL 6.x or 7.x

```
binutils-2.20.51.0.2-5.11.el6 (x86_64)
compat-libstdc++-33-3.2.3-69.el6 (x86_64)
compat-libstdc++-33-3.2.3-69.el6.i686
gcc-4.4.4-13.el6 (x86_64)
gcc-c++-4.4.4-13.el6 (x86_64)
glibc-2.12-1.7.el6 (i686)
glibc-2.12-1.7.el6 (x86_64)
glibc-common
glibc-devel-2.12-1.7.el6 (x86_64)
glibc-devel-2.12-1.7.el6.i686
libgcc-4.4.4-13.el6 (i686)
libgcc-4.4.4-13.el6 (x86_64)
libstdc++-4.4.4-13.el6 (32-bit and x86_64)
libstdc++-devel-4.4.4-13.el6 (32-bit and x86_64)
libstdc++-devel-4.4.4-13.el6.i686 (32-bit and x86_64)
libaio-0.3.107-10.el6 (32-bit and x86_64)
libaio-devel-0.3.107-10.el6 (32-bit and x86_64)
make-3.81-19.el6
sysstat-9.0.4-11.el6 (x86_64)
libXau.i686
libxcb.i686 include as it is.
libX11.i686
libXtst.i686
libXi.i686
libXext.i686
unixODBC (32 bit and 64-bit)
unixODBC-devel
```

#### On SUSE Linux Enterprise Server 11

```
make-3.81
binutils-2.19
gcc-4.3
libaio-0.3.104
libaio-devel-0.3.104
glibc-2.9
glibc-devel-2.9
libstdc++33-3.3.3
libstdc++43-4.3.3
libstdc++43-devel-4.3.3
sysstat-8.1.5
unixODBC-2.2.12 or later
unixODBC-devel-2.2.12 or later
unixODBC-32bit-2.2.12 (32 bit) or later
unzip.x86_64
```

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

- 4 Open the ports listed in the [“Protecting ArcSight Manager” on page 22](#) to facilitate a smooth communication between the ArcSight Manager and the database.



Red Hat Linux has firewall enabled by default, which causes the ESM setup and configuration programs to fail. Since ArcSight Manager needs to communicate with the database machine, open the ports listed in the [“Protecting ArcSight Manager” on page 22](#) on the ArcSight 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 to select at least the “default” package group option while configuring your RHEL 64-bit system.
- 9 Make sure that the location of the Archive Directory has enough space for archiving.
- 10 Set Shell Limits for the oracle User:
  - a Add the following lines to the `/etc/security/limits.conf` file, if they do not already exist:
 

```
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft nofile 1024
oracle hard nofile 65536
oracle soft stack 10240
```
  - b Add the following line to the `/etc/pam.d/login` file, if it does not already exist:
 

```
session required pam_limits.so
```

## 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” on page 33](#).
- 2 ESM 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.
- 4 Make sure that the location of the Archive Directory has enough space for archiving.

## Installing ArcSight Database



**Caution**

Run tools that require a remote login to a Manager in FIPS mode 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.



**Note**

- A Windows system was used for the sample screens. Path separators are / for Linux and \ for Windows.
- Use the ArcSight Database installer to create an Oracle instance and the ArcSight schema.
- ArcSight Database is supported on 64-bit platforms only.

The installation 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 with Oracle 11g
  - ◆ A new ArcSight Database installation that uses pre-existing Oracle 11g software

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



**Note**

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

```
arcsight databasesetup
```

## 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 the ArcSight Database component and, if needed, the Oracle database software.

Follow these steps to install the ArcSight Database software:

- 1 Download the ArcSight Database installation file, and if needed, the Oracle 11g database files appropriate for your platform from the HP SSO Download site. Copy all the files (without extracting their contents) to a temporary directory.



**Caution**

Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

The following Oracle install files are available.

Platform	Oracle 11g Database Files
Windows	AMD64: p13390677_112040_MSWIN-x86-64_1of7.zip p13390677_112040_MSWIN-x86-64_2of7.zip
Linux	AMD64: p13390677_112040_Linux-x86-64_1of7.zip p13390677_112040_Linux-x86-64_2of7.zip



Note

The above file names indicate that there are seven Oracle binary files available for each platform, but only two filenames are listed in the table against each platform. This is because ESM includes only those Oracle binaries that are relevant to ArcSight Database.

Platform	ArcSight Installation file
Windows	ArcSight-5.6.x.nnnn.y-DB-Win.exe
Linux	ArcSight-5.6.x.nnnn.y-DB-Linux.bin

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party. Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

- 2 Run the appropriate self-extracting ESM installation file for your platform. On Linux, set the `LC_ALL` environment variable first by running the following command (and then run the installer from the same shell):

```
export LC_ALL=[language].UTF-8
```

...where [language] is one of these:

```
en_US (English)
zh_CN (Simplified Chinese)
zh_TW (Traditional Chinese)
ja_JP (Japanese)
fr_FR (French)
ko_KR (Korean)
ru_RU (Russian)
```



Note

A Windows system was used for the sample installation. If you are installing your database on a Linux based system, the screens may have a different appearance.

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 In the License Agreement screen, read the agreement text and click **I accept the terms of the License Agreement** radio button and click **Next**. This radio button is disabled until you scroll to the bottom of the agreement.

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

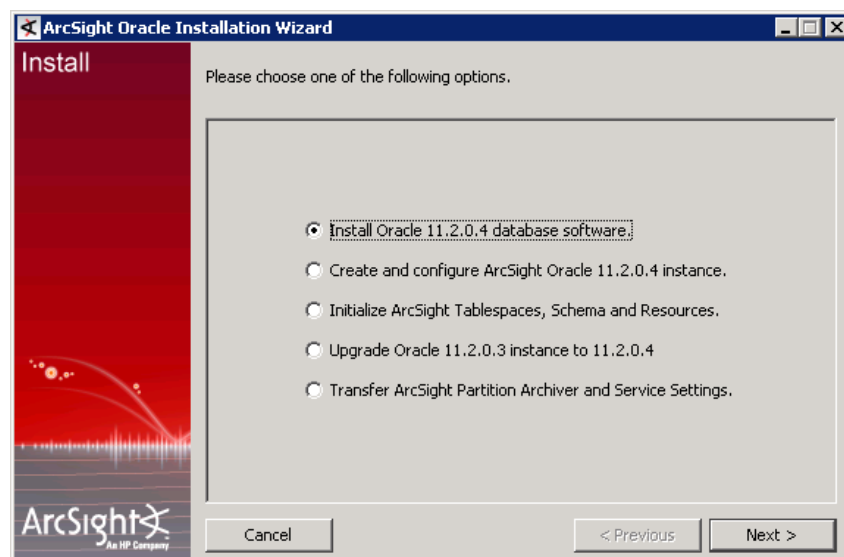


If the directory you choose already exists, the installer clears it. If you do not want to delete the existing contents of the directory, specify a new location for the current installation.

- 7 Select a folder in which to create the product icon.
- 8 Check to make sure that the folder locations in the Pre-installation Summary are correct and click **Install**.

A screen showing the progress of the installation appears. The Oracle configuration wizard opens after the installation is complete.

- 9 In the following screen, select from one of the following options.



If you are installing ArcSight Database for the very first time and do not have Oracle 11g pre-installed on your machine, select the **Install Oracle 11.2.0.4 database software** option. Go to ["Installing Oracle 11g Database Software" on page 48](#) for instructions to install Oracle 11g.

If you have a pre-existing Oracle 11.2.0.4 installation on your machine, create an Oracle 11g instance by selecting the **Create and configure ArcSight 11.2.0.4 instance** option. Go to ["Creating a New Oracle 11g Instance" on page 52](#) for detailed instructions on creating an Oracle 11g instance.

To use an existing Oracle 11g software installation with an existing Oracle 11g instance, choose the **Initialize ArcSight Tablespaces, Schema and Resources** option. Go to ["Initializing ESM Tablespaces, Schema, and Resources" on page 59](#) section for more information on initializing tablespaces, schema, and resources.



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

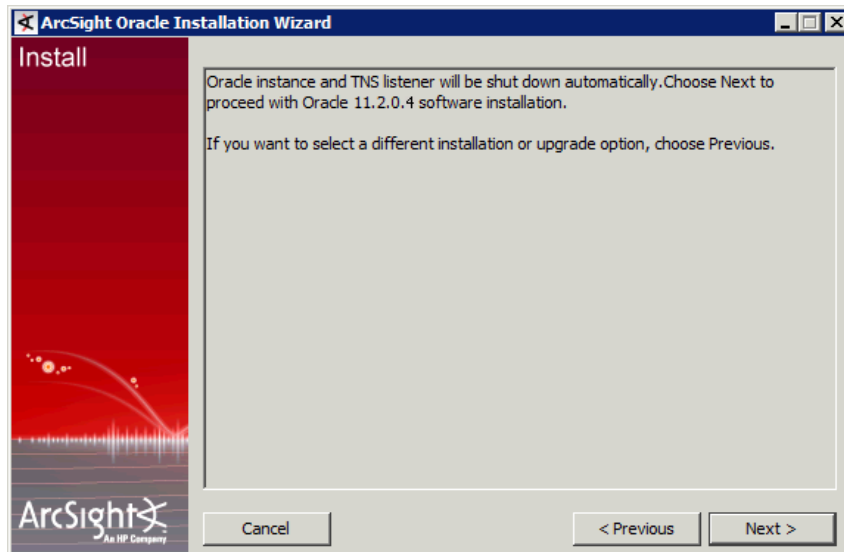
```
arcsight databasesetup
```

ESM v5.6 does not support Oracle 10g. If you are using Oracle 10g, you must upgrade your Oracle instance to 11g. You can do so using the ESM v5.0 SP2 ArcSight Database installer. Follow the instructions in the ESM Upgrade Guide for v5.0 SP2 to upgrade your Oracle software.

You can ignore the **Transfer ArcSight Partition Archiver and Service Settings** option. This option is used to transfer Partition Archiver settings from an existing installation and is only applicable if you are upgrading ArcSight Database.

## Installing Oracle 11g Database Software

- 1 The following screen prompts you to shut down currently running Oracle instances or TNS listeners. If this is a fresh installation, skip this step.



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.

```
% arcdbutl lsnrctl stop
```

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

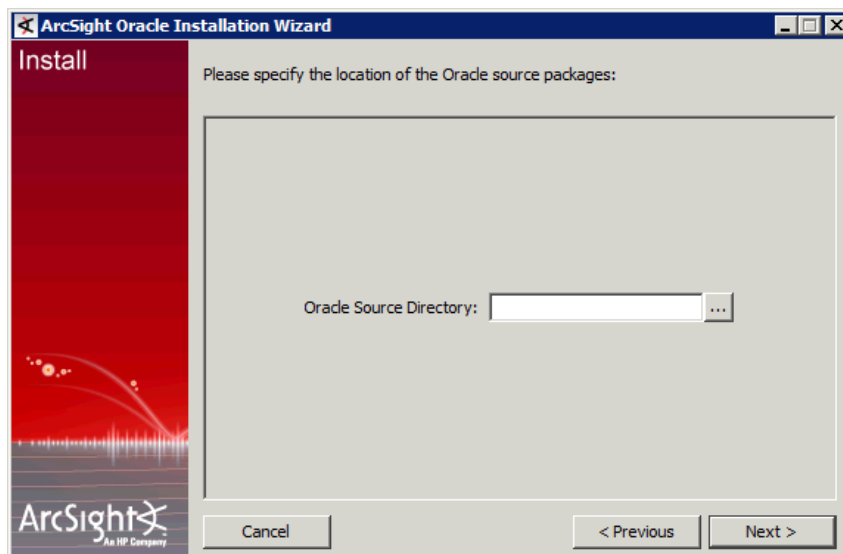
```
% arcdbutl sql
```

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

```
SQL> shutdown immediate
```

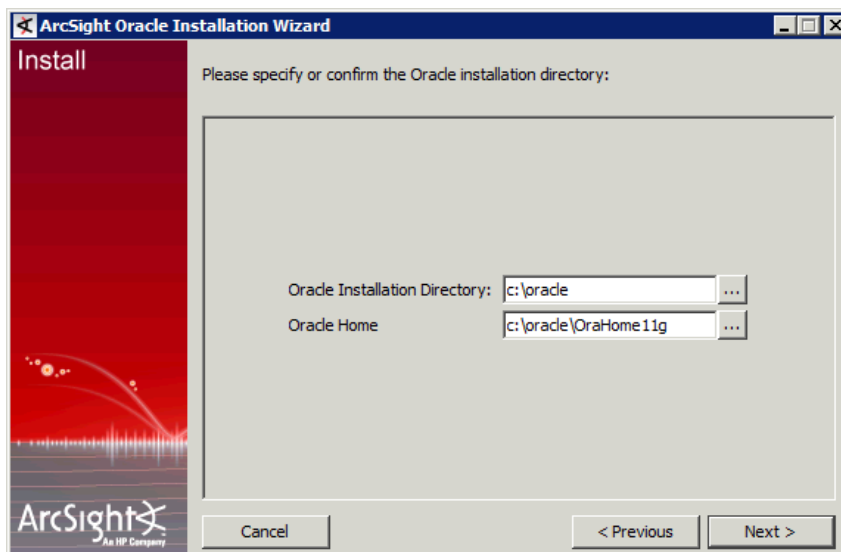
```
SQL> exit
```

- 2 Enter the location where you copied the Oracle 11g database software files in Step 1 of ["Installing the ArcSight Database Software" on page 45](#) and click **Next**:

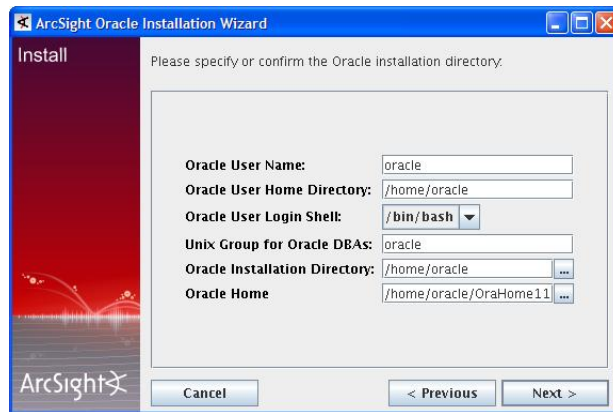


- 3 Specify a new one or confirm the default Oracle installation directory and click **Next**:

On Windows:



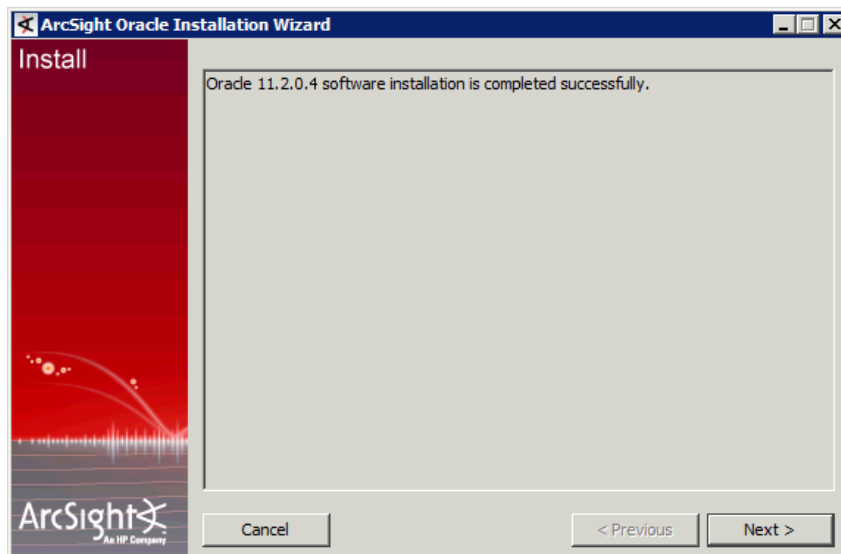
On Linux:



Verify that the Oracle installation directory path and the Oracle home path do not contain any spaces.

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

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



If you are on a Linux system, make sure to follow the instructions in the [Configuring Shared Memory on Linux](#) section before proceeding further.

## Configuring Shared Memory on Linux

Before creating the database instance on a Linux fresh install system, make sure you have enough shared memory on `/dev/shm` for the template you are planning to choose. This verification is required because you might not have enough shared memory; and if you proceed with database instance creation with inadequate shared memory, the Oracle database memory parameters are not set correctly.

To identify the available amount of shared memory on your system, check the size of `/dev/shm` from the Linux prompt by executing:

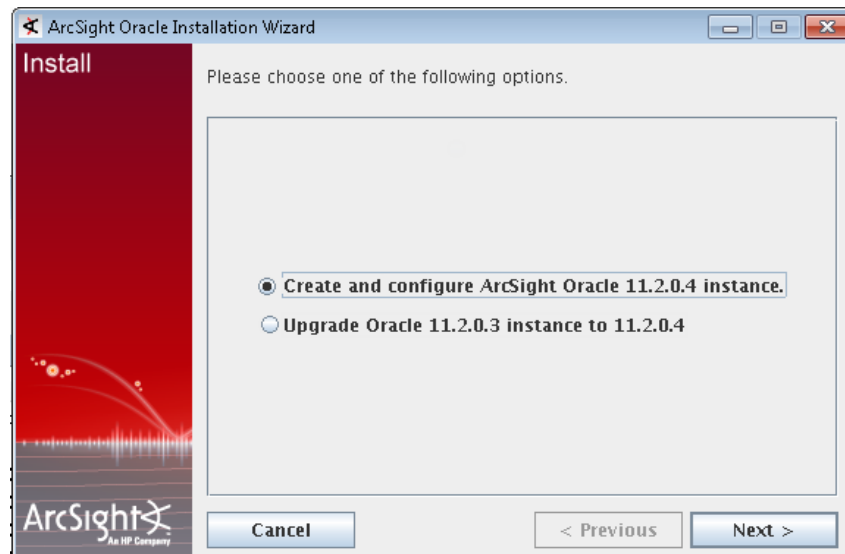
**df -k**

If shared memory is less than what you need, increase as required for your template creation using the following recommendations. Then proceed with the instance creation using the ArcSight Database software component.

The shared memory should be more than the following:

Template Size	Required Memory	Shared Memory Requirements
Small	246M	500M
Medium	740M	1G
Standard	1442M	3G
Large	2986M	4G
XLarge	6096M	7G
XXLarge	12160M	13G

- 5 Select "Create and configure ArcSight Oracle 11.2.0.4 instance" and click **Next**.



## Creating a New Oracle 11g Instance



**Setting the Database Block Size:** ArcSight embedded Oracle installer creates 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, 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\Oracle11g\<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, enter the following parameters in the next screen.

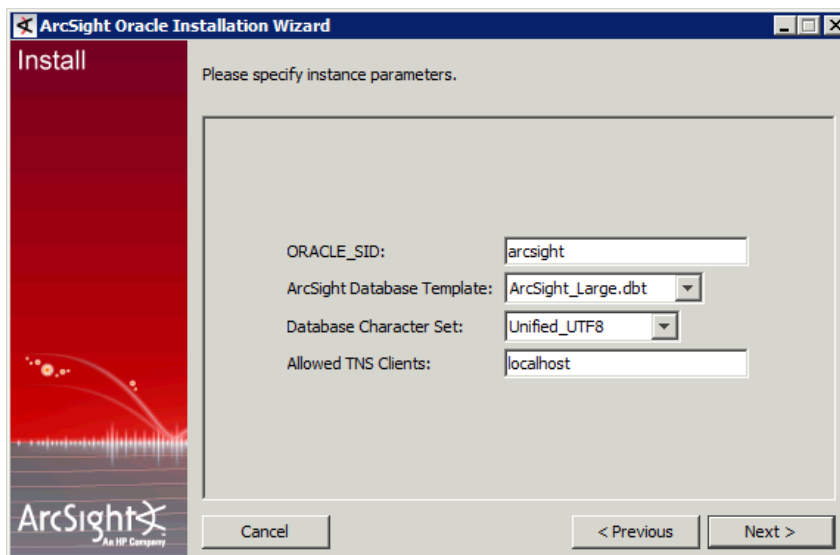
**ORACLE\_SID**—System ID (SID) for the ArcSight Database. By default, **arcsight**. The global database name and the TNS service name are set to the value you specify for this parameter. The Oracle SID cannot exceed 8 characters and must not contain any spaces. The Oracle SID is also the database instance name.

**ArcSight Database Template**—The template that determines the configuration (for example, memory allocation) of the ArcSight Database you want to create. By default, `ArcSight_Large.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 41](#).

**Database Character Set**—The language that Oracle should use to operate; for example, English. By default, the Database Character Set is `Unified_UTF8`.

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



**Note**

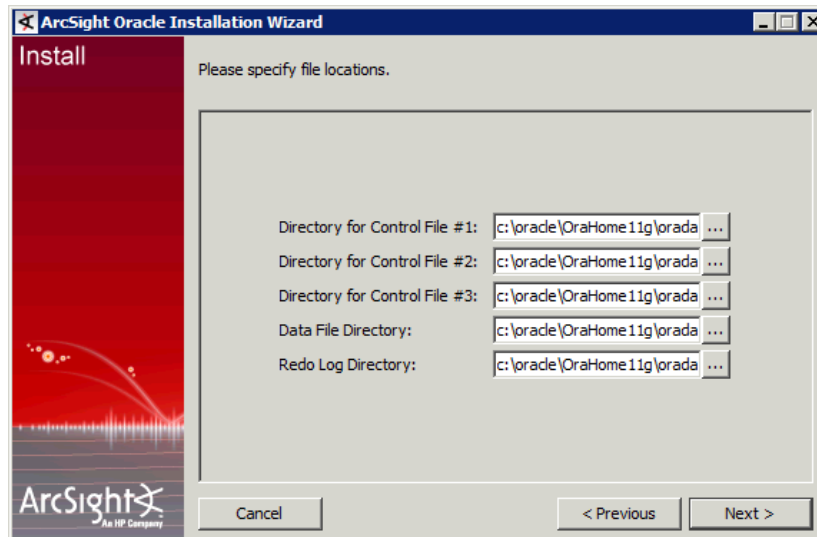
The database machine only accepts connection requests from the specified client list. If the ArcSight Manager is running on another host (as recommended), include both the 'localhost' and the ArcSight Manager host in the list. The installer automatically replaces 'localhost' with the actual IP address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

- 2 Enter the following parameters in the next screen. Although default directory locations are filled for you, we recommend 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 are 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 are stored. By default, <ORACLE\_HOME>\oradata\ORACLE\_SID.



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

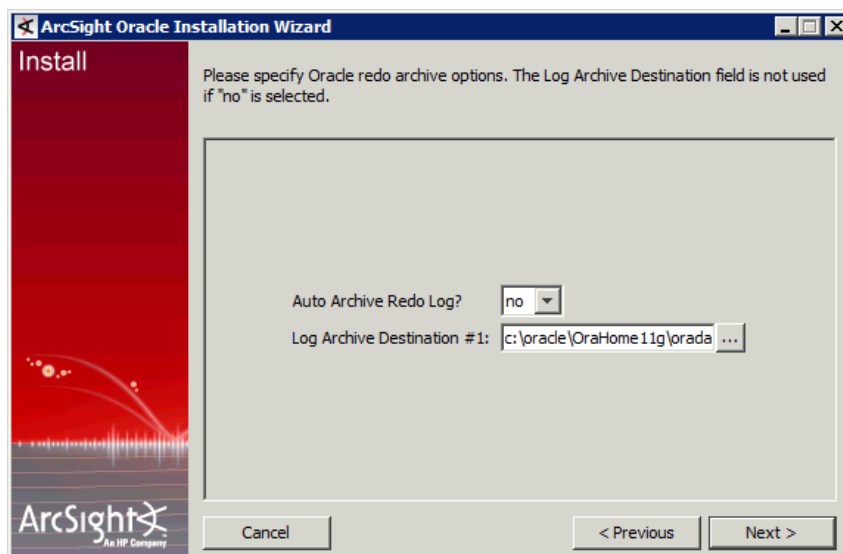
**Auto Archive Redo Log**-- Specify whether to enable automatic log archiving. Note that Redo log archiving requires a large amount of additional disk space and it impacts database performance. Only enable log archiving in situations where you cannot tolerate any loss of data from disk crashes. By default, 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.



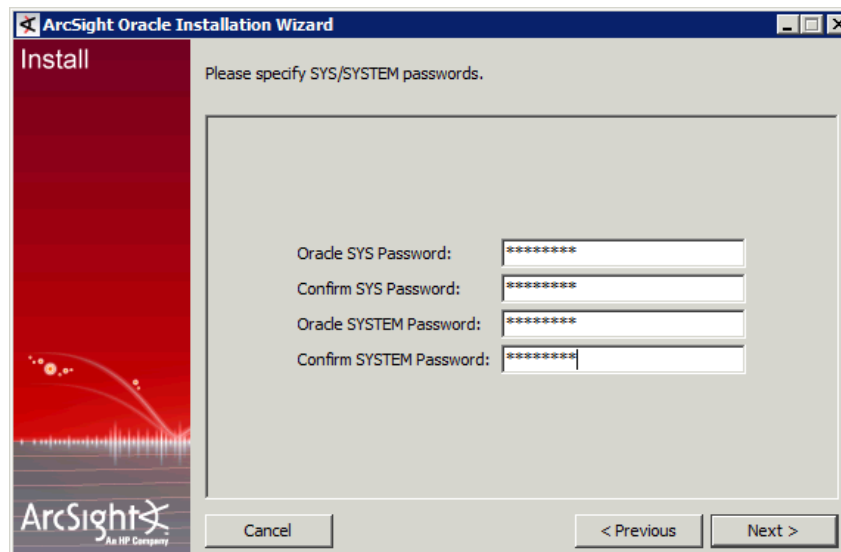
The log archive destination cannot be on a raw disk partition.



- 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:



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 ESM's Oracle 11g Installer, you must acquire licensing and support from Oracle directly.

ArcSight Oracle Installation Wizard

Install

Please specify Enterprise Manager options. The password fields are not used if "no" is selected.

Install Enterprise Manager ? no

Oracle DBSNMP Password:

Confirm DBSNMP Password:

Oracle SYSMAN Password:

Confirm SYSMAN Password:

Cancel < Previous Next >

Click **Next** to continue.

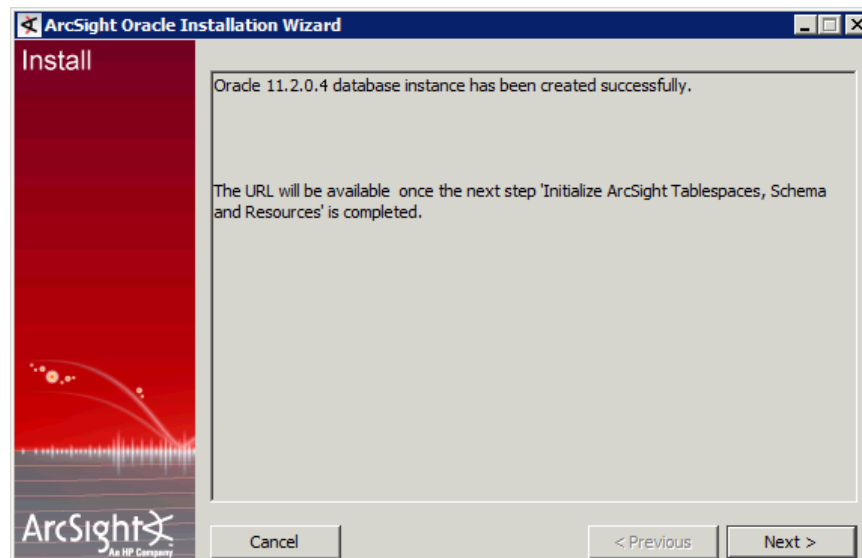
ArcSight Oracle Installation Wizard

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 >



Note

If you opted to install the Oracle Enterprise Manager (OEM), you can access the OEM URL once the OEM starts. This URL should be as follows:  
<https://<hostname>:1158/em>.

## Verify Memory\_Target

After you complete the instance creation, do the following to verify if the instance was created with the correct parameters by running these commands on the database machine:

```
arcdbutil sql / as sysdba

show parameter memory_target
```

The `memory_target` value should be the same as the required memory specification in the following table for the chosen template. If it is correct, then you are done.

Template Size	Required Memory
Small	246M
Medium	740M
Standard	1442M
Large	2986M
XLarge	6096M
XXLarge	12160M

If `memory_target` is set to zero, run the following:

```
alter system set sga_target=0 scope=spfile;

alter system set pga_aggregate_target=0 scope=spfile;
```

```

alter system set memory_target=<required_memory_for the
template_used> scope=spfile;

shutdown immediate

startup

show parameter memory_target;

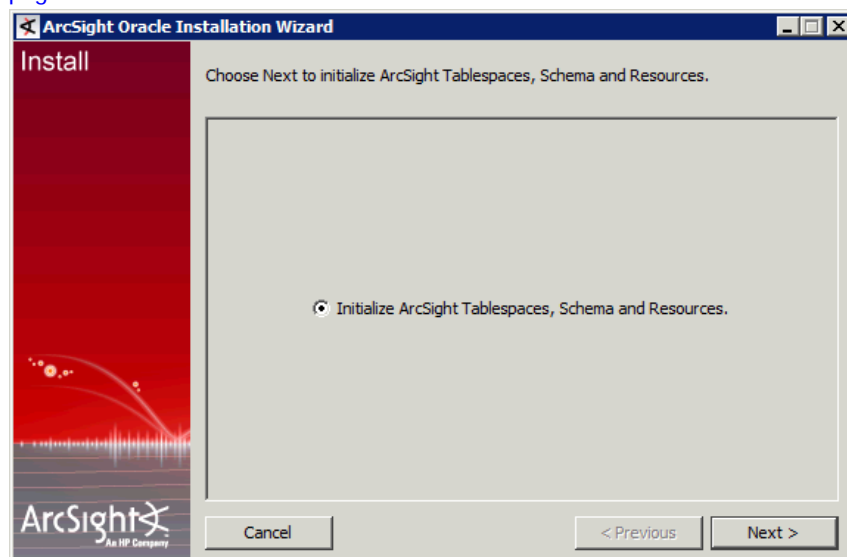
show parameter sga;

show parameter pga_aggregate_target;

exit

```

- 6 Click **Next** to start initializing ESM tablespaces, schema, and resources. Follow the procedure described in [“Initializing ESM Tablespaces, Schema, and Resources” on page 59](#).



## Avoiding DB Write Performance Issues with Oracle 11g

During fresh installations after creating the DB instance, you may need to modify the Oracle initialization parameter “log\_buffer” in case you encounter problems with database write performance.

### To modify the log\_buffer parameter:

- 1 At the prompt, enter  
**arcdbutil sql**
- 2 As user name, enter:  
**/ as sysdba**
- 3 At the SQL prompt, enter:  
**show parameter log\_buffer**  
The value is set to a value around 1 MB.
- 4 Modify the log\_buffer value to 14 MB:

```
alter system set log_buffer=14237696 scope=spfile
```

- 5 Shut down the Oracle instance for the changes to take effect. At the prompt, enter:

```
shutdown immediate
```

```
startup
```

- 6 To verify that the log buffer was reset correctly enter:

```
show parameter log_buffer
```

The system should display **14237696**.

- 7 At the prompt, enter **exit**.

## Initializing ESM Tablespaces, Schema, and Resources

- 1 You must check the status of the TNS listener and Oracle 11g 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:

On Linux

```
% arcdbutil lsnrctl start
```

On Windows, you can either start the TNS listener from Windows Services or run the above command from a DOS prompt.

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
```

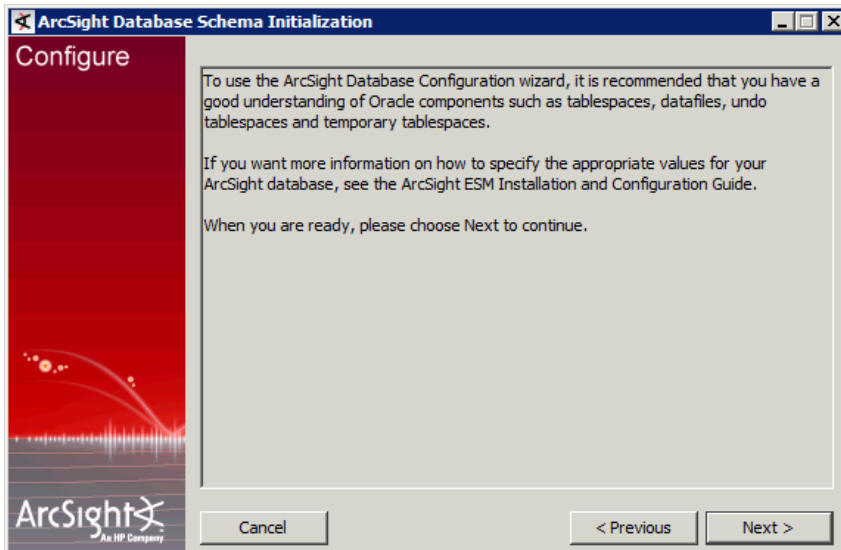
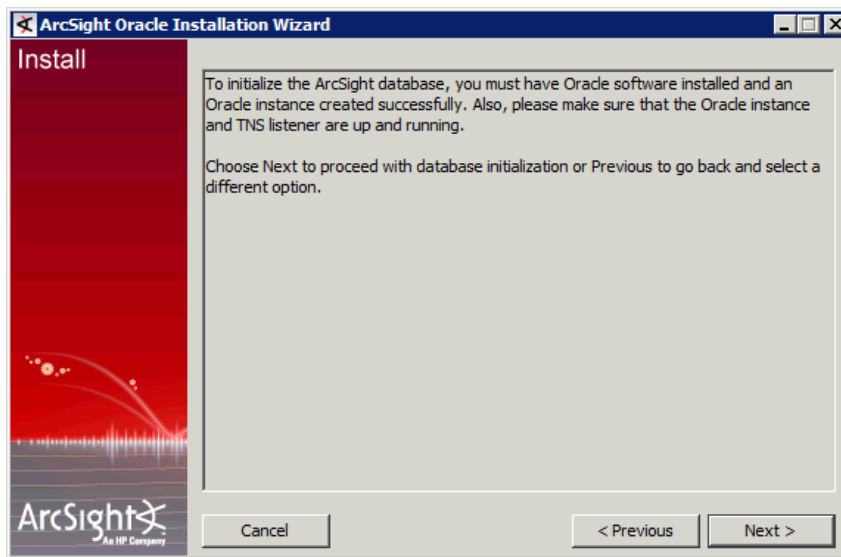
To start the Oracle instance, run this command on the database machine:

```
% arcdbutil sql
```

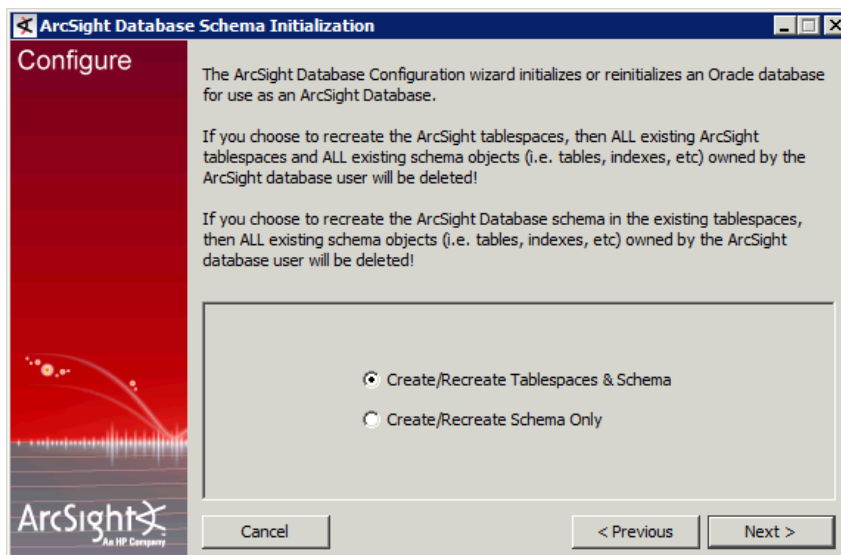
```
Enter user-name: / as sysdba
```

```
SQL> startup
```

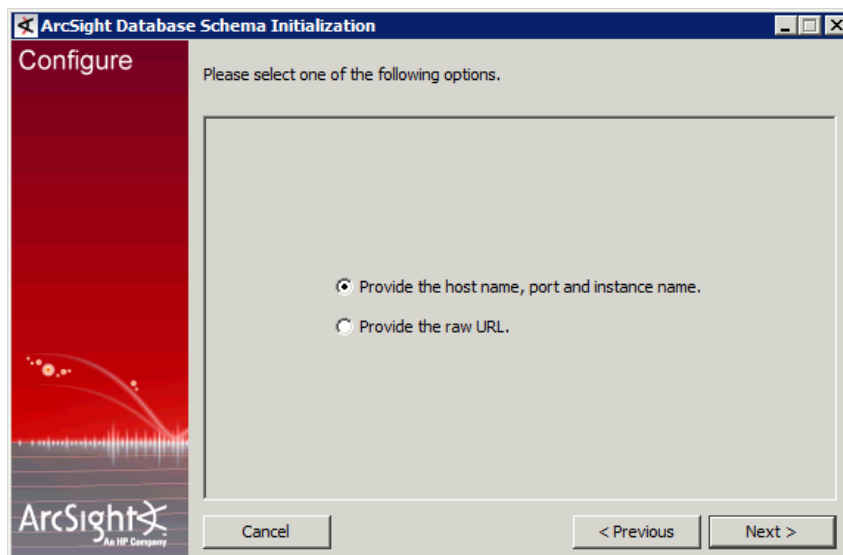
```
SQL> exit
```



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

Keep in mind that Oracle supports only alphanumeric characters for database user names, and cannot accept a dash (-) or underscore (\_) in these names.

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

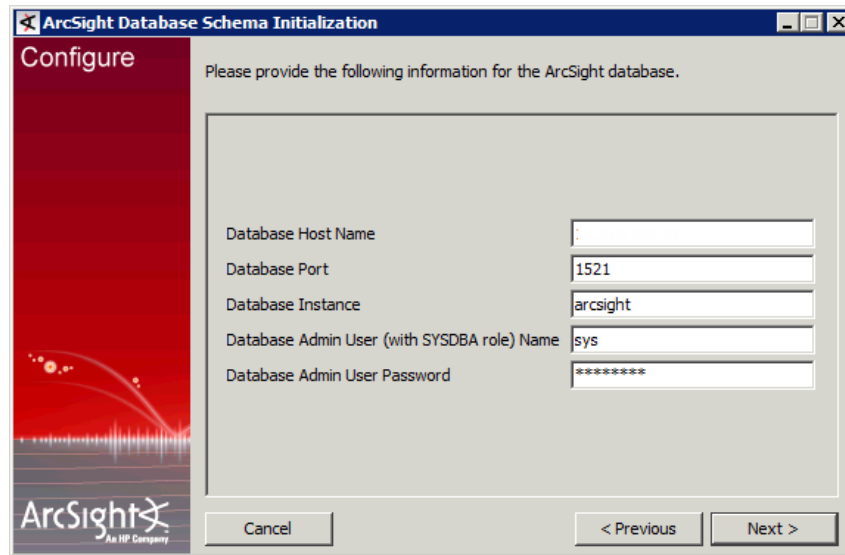
**Database Port**—The TCP port number on which the Oracle listener listens for connections. By default, 1521.

**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.

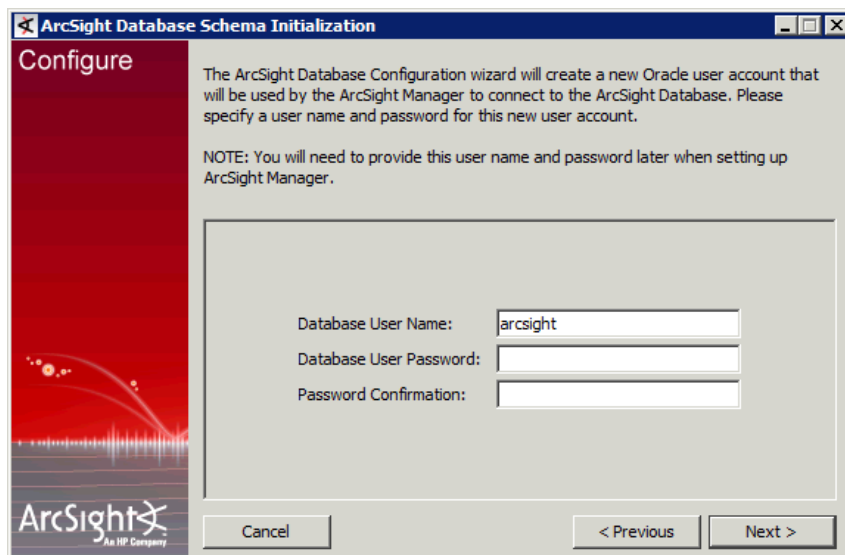
**Database Admin User Password**—The password for the Oracle super user account.

**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, 'Configure' tab. The title bar says 'ArcSight Database Schema Initialization'. The left sidebar has the ArcSight logo and 'Configure'. The main area says 'Please provide the following information for the ArcSight database.' Below this are five input fields: 'Database Host Name' (empty), 'Database Port' (1521), 'Database Instance' (arcsight), 'Database Admin User (with SYSDBA role) Name' (sys), and 'Database Admin User Password' (masked with asterisks). At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

- 5 Enter a Database User Name and User Password and click **Next**.



The screenshot shows the 'ArcSight Database Schema Initialization' window, 'Configure' tab. The title bar says 'ArcSight Database Schema Initialization'. The left sidebar has the ArcSight logo and 'Configure'. The main area says '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: You will need to provide this user name and password later when setting up ArcSight Manager.' Below the note are three input fields: 'Database User Name:' (arcsight), 'Database User Password:', and 'Password Confirmation:'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

- 6 The next screen prompts you to enter a name for System User.

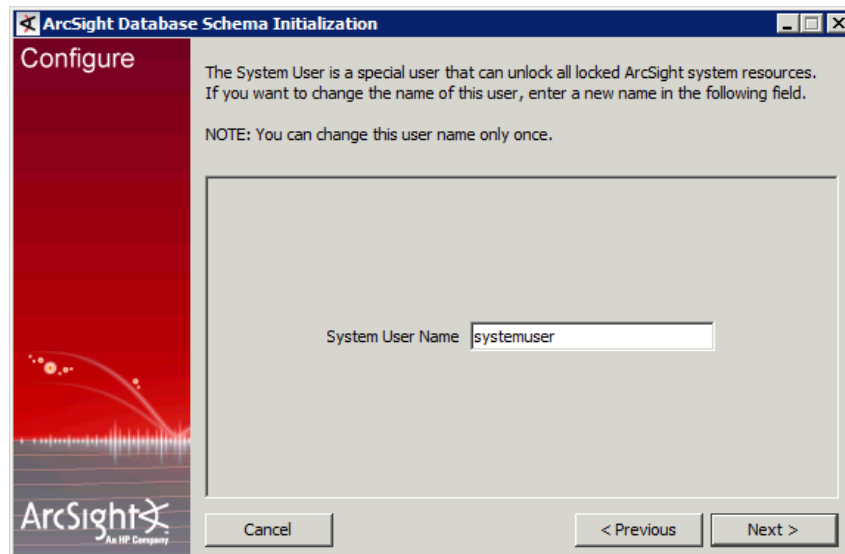
During the installation process, a set of predefined content called the System Core content is installed by default. This content provides the foundation building blocks for the ESM system to work.

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 ESM, therefore, it is locked by default. We strongly recommend 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. We recommend 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 37](#).

Enter the following information for each tablespace:

**Data File Path**—The directory where the data files for this tablespace are 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.

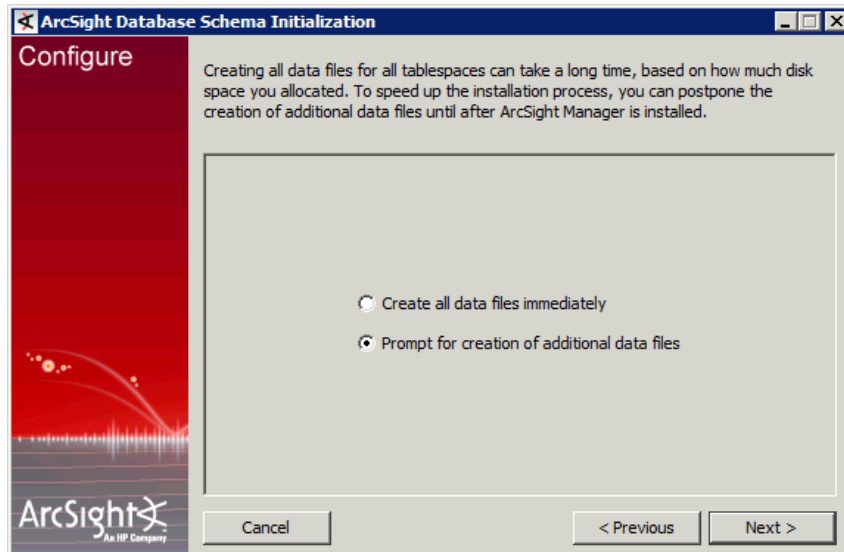
**Number of Data Files**—The number of data files created for the tablespace.

A large number of long-running queries might require a larger ARC\_UNDO tablespace. No recommendation can work for all users.

- 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. We recommend 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.



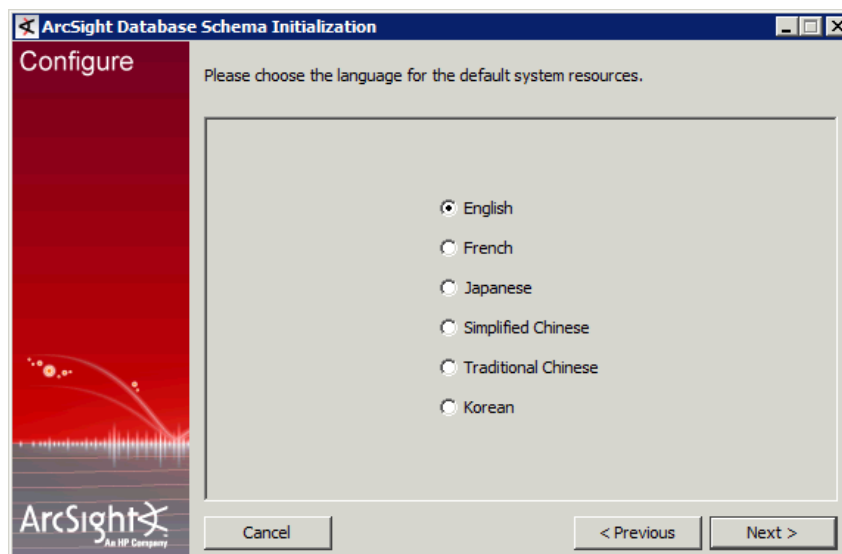
- 9 In [Step 1 on page 52](#) if you had chosen a database character set that supports more than one language supported by ESM, you see the following screen requesting you to select a language for installing your system resources in:



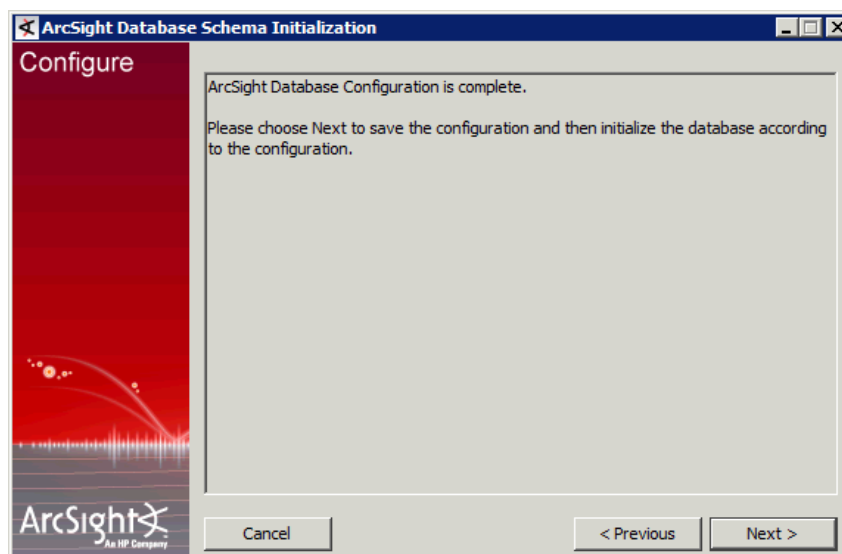
**Note**

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

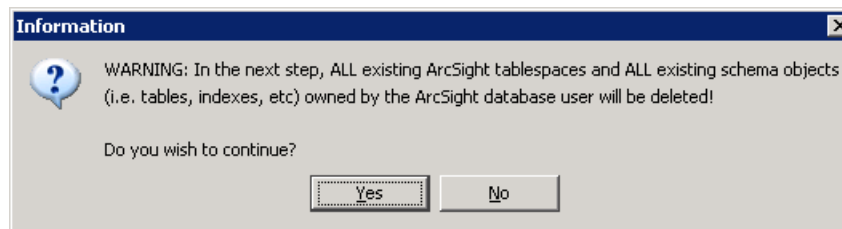
Not all languages listed here are supported. Refer to the ESM Release Notes for the languages that are supported for this release.



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

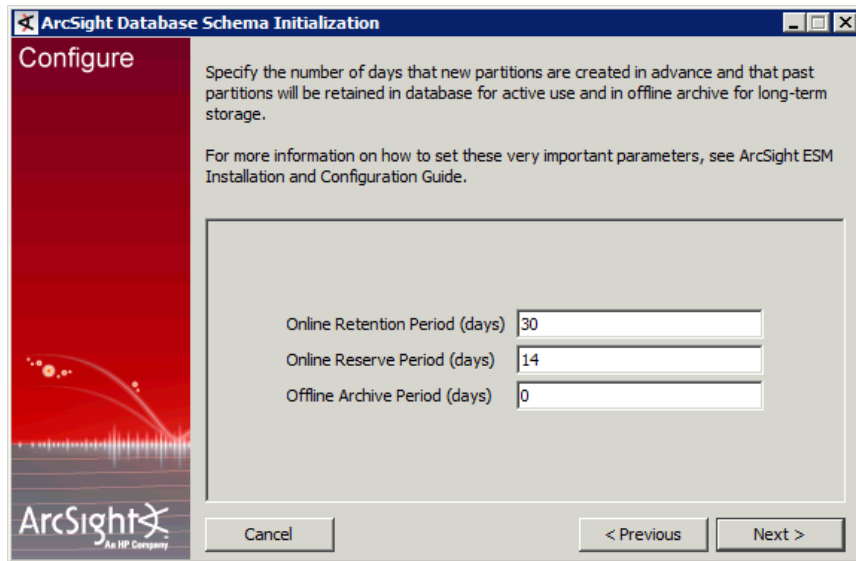


You see the following warning message.



To initialize the database schema, specify the parameters in the next few screens. For more information about these parameters, see ["Configuring Partition Management" on page 71](#)

- 11 Specify the partition retention information. Partitions are 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 with the 'Configure' tab selected. The window title is 'ArcSight Database Schema Initialization'. The left sidebar has the 'Configure' tab highlighted. The main content area has a red background on the left with the ArcSight logo and a white area on the right with instructions and input fields. The instructions state: '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 ESM Installation and Configuration Guide.' The input fields are: 'Online Retention Period (days)' with value '30', 'Online Reserve Period (days)' with value '14', and 'Offline Archive Period (days)' with value '0'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

**ArcSight Database Schema Initialization**

**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 ESM Installation and Configuration Guide.

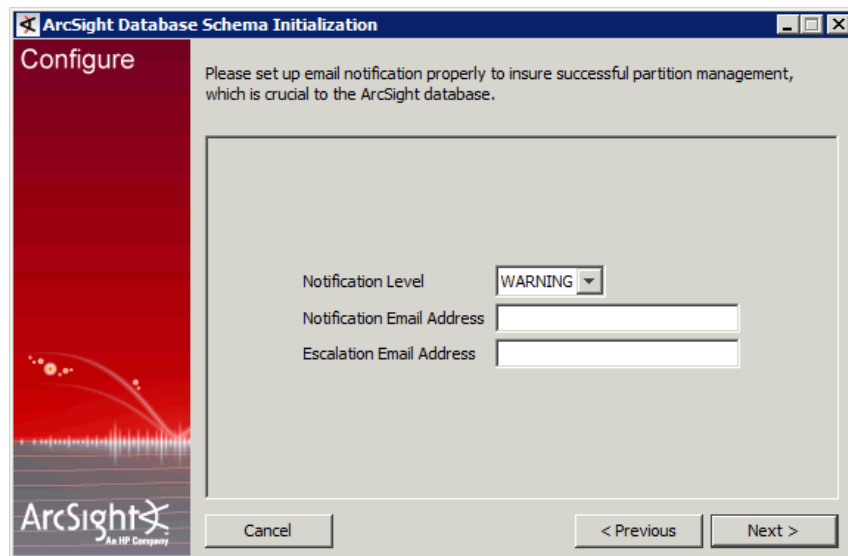
Online Retention Period (days)

Online Reserve Period (days)

Offline Archive Period (days)

Cancel < Previous Next >

- 12 Enter the e-mail notification to be sent if the Partition Manager encounters a problem.



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 the 'Configure' tab highlighted. The main content area has a red background on the left with the ArcSight logo and a white area on the right with instructions and input fields. The instructions state: 'Please set up email notification properly to insure successful partition management, which is crucial to the ArcSight database.' The input fields are: 'Notification Level' with a dropdown menu showing 'WARNING', 'Notification Email Address' with an empty text box, and 'Escalation Email Address' with an empty text box. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

**ArcSight Database Schema Initialization**

**Configure**

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

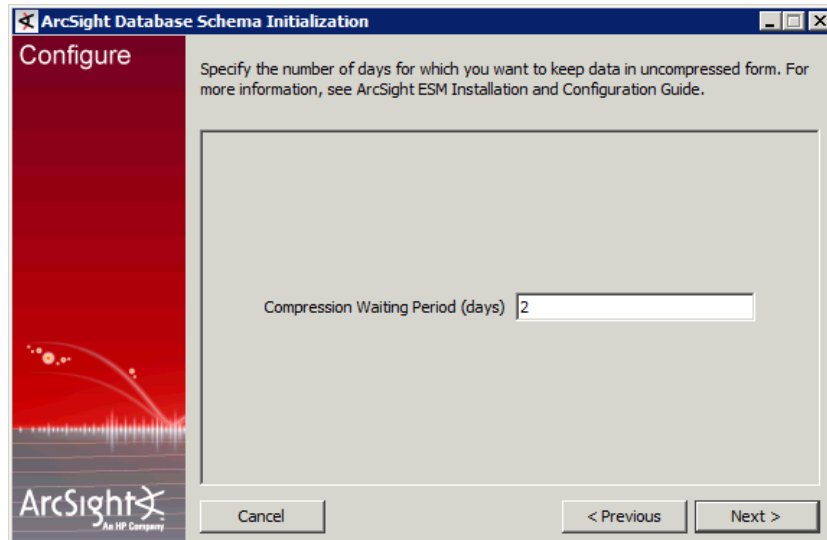
Notification Level

Notification Email Address

Escalation Email Address

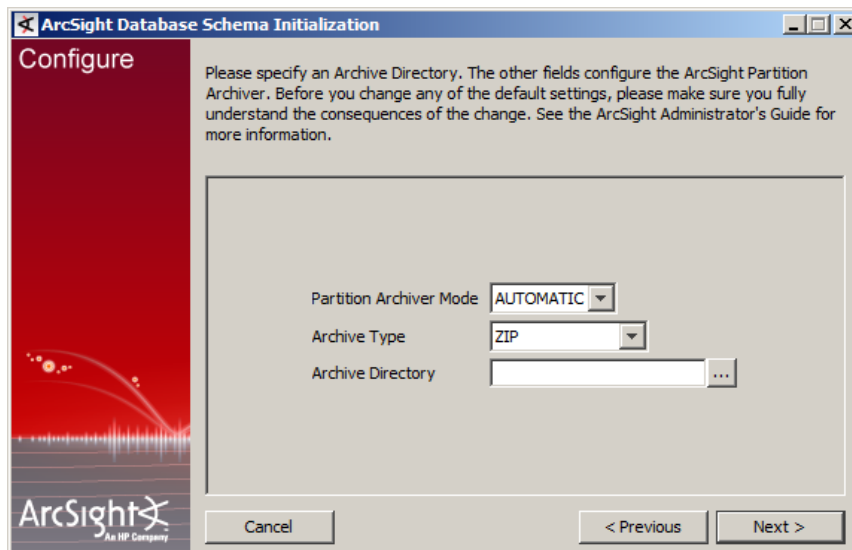
Cancel < Previous Next >

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

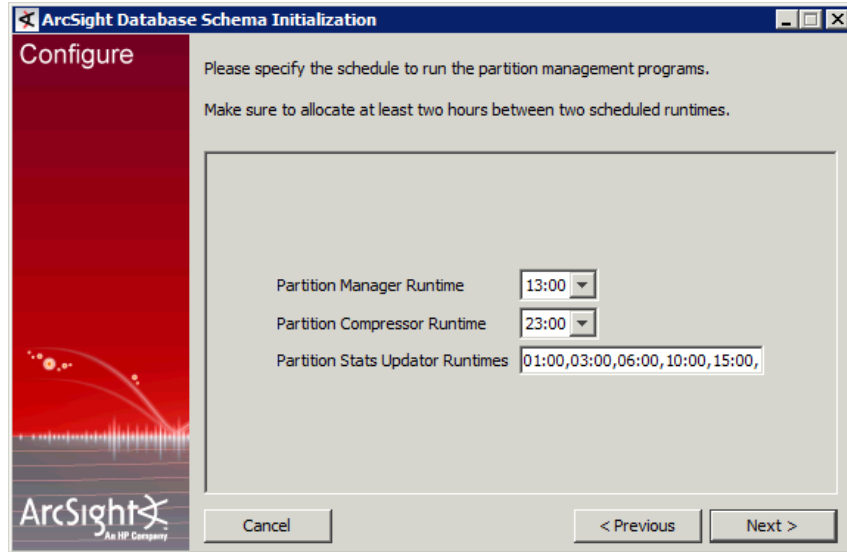


- 14 The next screen prompts you to enter or select the Partition Archiver mode, archive type, and archive directory. If you are using SUSE 11, do not select the ZIP Archive Type, as it is not supported on that platform.

Make sure that your archive directory is placed in a location that has enough disk space for archiving.



- 15 Schedule the partition management programs. The Partition Manager runs only once in 24 hours, and you can configure that time in the following panel.



The screenshot shows the 'ArcSight Database Schema Initialization' window with the 'Configure' tab selected. The window has a red sidebar with the ArcSight logo. The main area contains instructions: 'Please specify the schedule to run the partition management programs. Make sure to allocate at least two hours between two scheduled runtimes.' Below this are three configuration fields: 'Partition Manager Runtime' set to 13:00, 'Partition Compressor Runtime' set to 23:00, and 'Partition Stats Updator Runtimes' with a text box containing '01:00,03:00,06:00,10:00,15:00,'. At the bottom are 'Cancel', '< Previous', and 'Next >' buttons.

ArcSight Database Schema Initialization

Configure

Please specify the schedule to run the partition management programs.  
Make sure to allocate at least two hours between two scheduled runtimes.

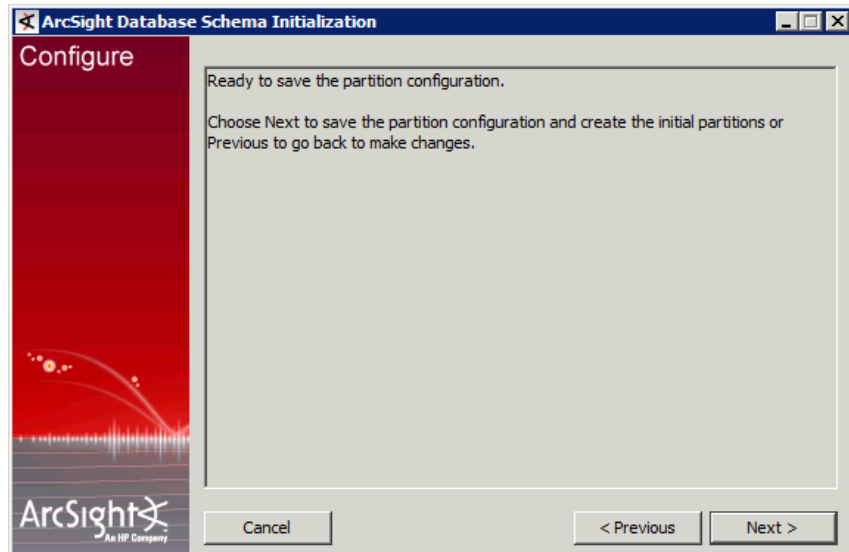
Partition Manager Runtime 13:00

Partition Compressor Runtime 23:00

Partition Stats Updator Runtimes 01:00,03:00,06:00,10:00,15:00,

Cancel < Previous Next >

Click **Next**.



The screenshot shows the same 'ArcSight Database Schema Initialization' window, but the text in the main area has changed to: 'Ready to save the partition configuration. Choose Next to save the partition configuration and create the initial partitions or Previous to go back to make changes.' The configuration fields and buttons remain the same.

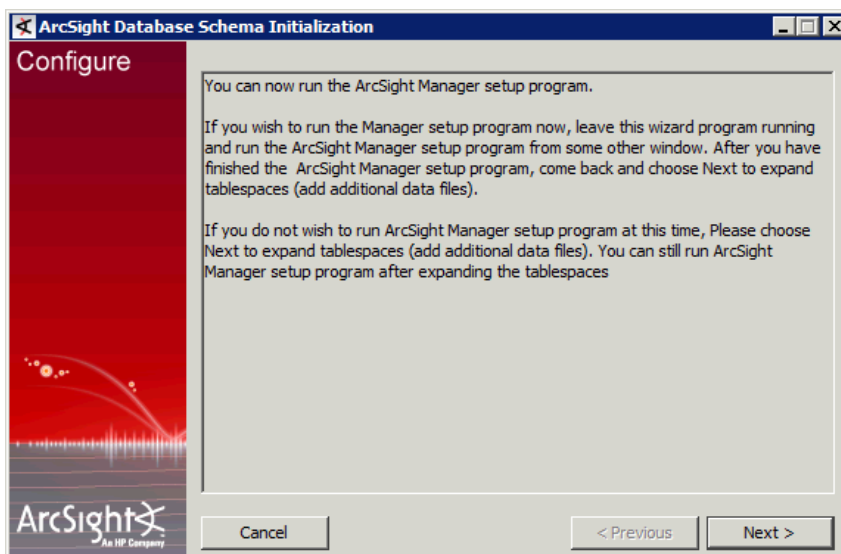
ArcSight Database Schema Initialization

Configure

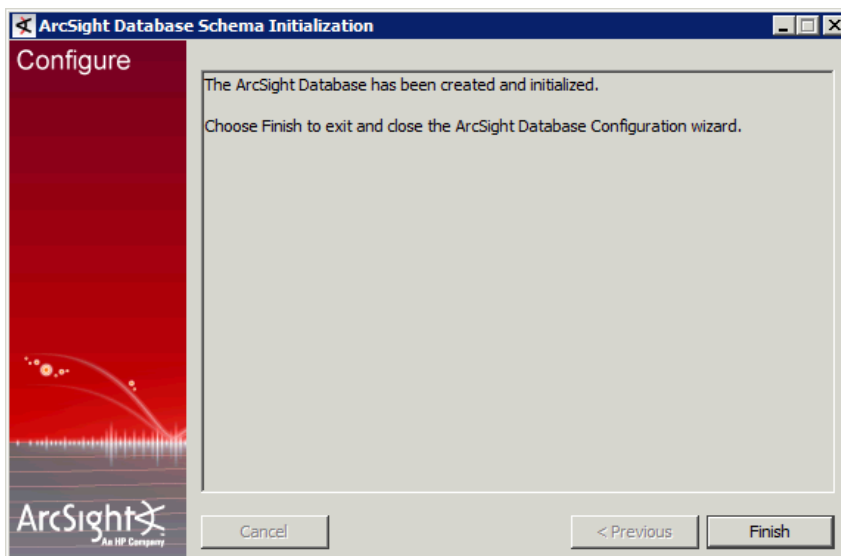
Ready to save the partition configuration.  
Choose Next to save the partition configuration and create the initial partitions or  
Previous to go back to make changes.

Cancel < Previous Next >

Click **Next**.



You have installed the Oracle 11g database and the ArcSight Database component. Click **Finish** in the following screen:



Click **Done** in the last screen.

- 16** 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.

- 17** Starting with 11g, by default, Oracle has set the passwords to expire 180 days after the account has been created. This causes connectivity issues to the database after the 180 day default period on both new installs as well as on upgraded systems.

If you run into this problem of expired password, then do the following to set the password to never expire.

- a** % arcdbutil sql
- b** Enter user-name: / as sysdba
- c** SQL> select PROFILE from dba\_users where username =  
'<arcsight\_schema\_owner>';
- d** SQL> alter PROFILE <profile result from step 3> limit  
PASSWORD\_LIFE\_TIME UNLIMITED;
- e** SQL> exit;

In 11g, by default, Oracle has set the failed login attempts value to 10. If the account gets locked for exceeding the number of failed login attempts, use the following to resolve the issue.

- a** % arcdbutil sql
- b** Enter user-name: / as sysdba
- c** SQL> alter user <arcsight\_schema\_owner> account unlock;
- d** SQL> exit;

For more information on changing this behavior, refer to the Knowledge Centered Support (KCS) article KM1273029, which is available from the HP SSO portal at:

<http://support.openview.hp.com/selfsolve/document/KM1273029>



In you see an error in the log after this installatin that says: "Package "pdksh" is missing, " you may ignore it. The pdksh package is not actually required by Oracle, and is not provided by Red Hat.

## Restarting or Reconfiguring ArcSight Database



**On Linux systems only:** Oracle 11g installation on Linux requires that the SELinux is disabled. So, after installing the database, during subsequent restarts of your machine, you must run the following commands to disable the SELinux and ensure that SELinux has been disabled.

To disable SELinux:

- 1 Run the following from a prompt:

```
getenforce
```

You should see "Enforcing" in the output for the command.

- 2 Run the following command:

```
setenforce 0
```

This disables SELinux on your system.

To ensure that SELinux has been disabled:

- 3 Run the following again to ensure that SELinux has been disabled:

```
getenforce
```

If you see "Permissive" in the output, SELinux has been successfully disabled.

Here is a sample output when you run the commands above:

```
[root@Arch-RHEL5 ~]# getenforce
Enforcing
[root@Arch-RHEL5 ~]# setenforce 0
[root@Arch-RHEL5 ~]# getenforce
Permissive
[root@Arch-RHEL5 ~]#
```

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 databasesetup
```

Re-initialization deletes 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.

HP ArcSight offers advanced life-cycle management facilities for security-event data partitions as an optional feature. This feature fully automates the database partition

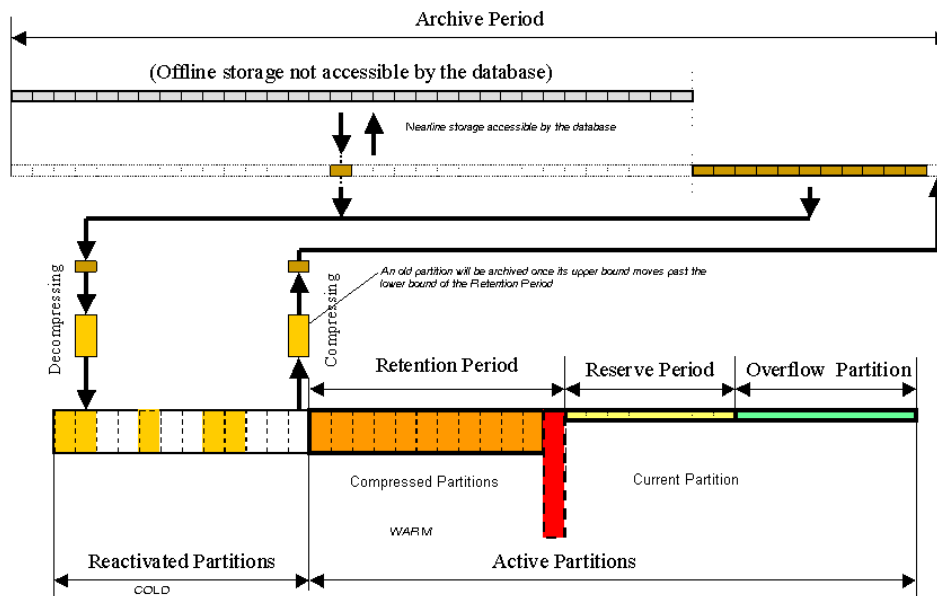
management process so that partitions containing old event data can be saved in offline archives automatically, and later be easily brought back online so security analysts can conduct forensic analyses using historical data from those archived partitions. This feature offers the ability to dramatically 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.

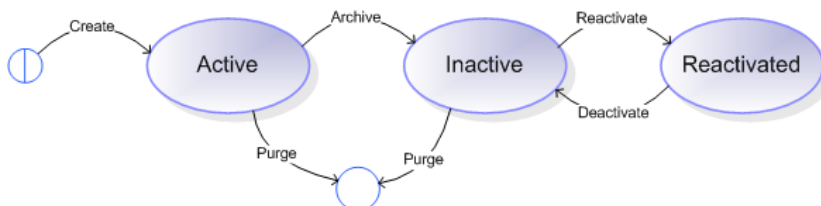
The following diagram illustrates the overall design for database partition management in the ArcSight Database when partition archiving is enabled.

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 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.



**Note**

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:

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

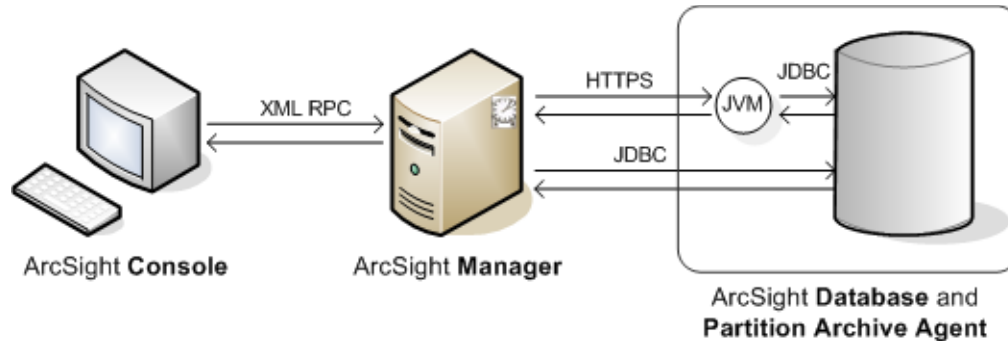
Successful partition management is crucial to database health and performance. Therefore, the Partition Manager should never be disabled for production systems.

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

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

If you set the Partition Archiver 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 sends 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" is 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 is then purged the next time Partition

Archiver runs. Normally, once the forensic analysis is completed, an administrative user manually deactivates 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 do not become effective until the ArcSight Manager is restarted. For example, the ArcSight 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"> <li>• Duration of task: Very Short</li> <li>• Initiated by Partition Manager in ArcSight Manager</li> <li>• Typically, takes a few seconds to one minute to create a new partition</li> </ul>
Retention Period	Dynamic	30 (days)	>=2 (See Note 1)	
Reserve Period	Dynamic	14 (days)	>=7	

Name	Type	Default Value	Valid Value	More Information
Partition Compressor Runtime	Static	23:00	00:30 - 23:30	<ul style="list-style-type: none"> <li>Duration of task: Long</li> <li>Initiated by Partition Compressor in ArcSight Manager</li> <li>CPU and I/O intensive</li> <li>Typically, takes one to two hours to complete (See Note 2)</li> </ul>
Compression Waiting Period	Dynamic	2 (days)	>=2	
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"> <li>Duration of task: Increases with each subsequent run</li> <li>Initiated by Partition Statistics Updater in ArcSight Manager</li> <li>CPU intensive</li> <li>Typically takes a few minutes for early runs and up to two hours for late runs (See Note 2)</li> </ul>
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"> <li>Duration of task: Long</li> <li>Executed by Partition Archiver on the database machine</li> <li>I/O intensive</li> <li>Typically takes up to two hours (See Note 2)</li> </ul>
Archive Period	Dynamic	0 (Days)	>=0	
Archive Type	Dynamic	ZIP - On Windows (see Note 5) GZIP - on Linux (See Note 3)	For Windows: ZIP, UNCOMPRESSED For Linux: ZIP, GZIP, BZIP2, UNCOMPRESSED (See Note 3)	UNCOMPRESSED, is not recommended.
Archive Directory	Dynamic	None	An existing directory to which the Oracle software owner has write privileges. (See Note 4)	

Name	Type	Default Value	Valid Value	More Information
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



- 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 is archived at once, make sure you have enough free space in the archive directory for it.
- 2 Duration depends on partition size, database configuration, and concurrent workload.
- 3 On Linux, GNU tar is available by default. Therefore, you do not need to do anything. If you do not want to install the GNU version of tar, select ZIP.
- 4 Create the Archive Directory in advance and give the Oracle software owner user full access to this directory. Make sure you have enough space in the file system/volume for this directory. We recommend 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 F, Installing ESM in FIPS Mode, on page 171](#).



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, change the `partitionarchiver.log` file owner from *root* to *oracle*.

Log in as the Oracle software owner (by default, *oracle* on Linux and *Administrator* on Windows) to configure Partition Archiver. The wizard configures Partition Archiver as a standalone application and registers 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

To run the `arcsight database pa` command or the `arcsight database pm` command in the remote mode on a Partition Archiver in FIPS mode, run these commands from the ArcSight Manager's `<ARCSIGHT_HOME>\bin` directory as opposed to the database `bin` directory.

- 3 Enter the ArcSight 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.

We recommend installing it as a service with the default values if possible. Run Partition Archiver as the Oracle software owner (Oracle, by default) on Linux and as a user (Administrator, by default) on Windows in the local user group `ORA_DBA`.

To install Partition Archiver as a service on Linux, run the following command as root:

```
<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.

On Windows, if the service does not start, it may be a privileges issue. To give privileges to a user group:

- 1 Go to **Control Panel > Administrative Tools > Local Security Policy**.
- 2 In the left pane, click on **Security Settings > Local Policies > User Rights Assignment**.
- 3 On the right pane click on the **Log On as a Service** policy.
- 4 Click **Add User or Group** and grant the right to the user who is to start the service.
- 5 Run the Partition Archiver setup again.

## 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 Linux 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
```

## 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 77](#).

## 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 Linux 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 Linux, 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 Linux and Administrator on Windows).
- 2 Run this command:

```
Linux: <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, neither the ArcSight Manager nor Partition Archiver can log in to the database. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration," "password Character Sets."

## Uninstalling the ArcSight Database Software

Stop ArcSight Database before uninstalling it.

Locate the <ARCSIGHT\_HOME>\UninstallerData folder and double-click:

```
Uninstall_ArcSight_DB.exe
```

To uninstall on Linux 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.



**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 Linux hosts, you can change the permissions to Read and Write for everyone (that is, 666).

---

## Chapter 3

# Installing ArcSight Manager

---

This chapter describes the installation and configuration of the Manager in default mode only. To install the Manager in FIPS mode, see [Appendix F, Installing ESM in FIPS Mode, on page 171](#). To install the Manager in FIPS with Suite B mode, see [Appendix F, Installing ESM in FIPS Mode, on page 171](#). Section “Differences Between Default and FIPS Modes” on [page 21](#) lists the basic differences between the three modes.



If you install the Manager in FIPS with Suite B mode, make sure that your SmartConnectors are also installed in FIPS with Suite B mode.

The following topics are covered in this chapter:

[“Manager Supported Platforms” on page 82](#)

[“Installing the Manager” on page 82](#)

[“Starting and Stopping the Manager” on page 108](#)

[“Verifying the Manager Installation” on page 110](#)

[“Reconfiguring Manager” on page 110](#)

[“Uninstalling Manager” on page 113](#)



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



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



Run tools that require a remote login to a Manager in FIPS mode 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.

## Manager Supported Platforms

**Note**

- While single-CPU and single-core systems are not supported, the Manager does support multiple-CPU and dual-core systems.
- A minimum of 4 GB RAM is required.

Refer to the Product Lifecycle document available on the Protect 724 website for the most current information on supported platforms. The machine hosting the Manager should be similar in capacity to the ArcSight Database host, because each processes 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 determines the number of concurrent ArcSight Console users and their perceived performance during peak event-per-second episodes. ArcSight 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

**Note**

A Windows system was used for the sample screens. If you are installing on a Linux based system, your screen may have a different appearance. Path separators are / for Linux and \ for Windows.

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

If you are using RHEL, then before you start, add the following line to your `/etc/profile` file:

```
export TZ='UTC'
```

To install Manager:

- 1 Download the ESM installation file appropriate for your platform from the HP SSO Download site (`ArcSight-5.6.x.nnnn.y-Manager-<platform>.zip`). Copy all the files (without extracting their contents) to a temporary directory.

**Caution**

Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party. Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

- 2 Extract the installation files from the compressed `ArcSight-5.6.x.nnnn.y-Manager-<platform>.zip` file.



- Installing ArcSight Web also requires you to extract its installation files from a compressed file. Installation files for ArcSight Web and Manager should be **not** be present in the same folder. So, make sure that you do **not** extract the Manager files into the folder where you plan to extract the ArcSight Web files.
- After unzipping, you get a `.exe` file (on Windows) or a `.bin` file (on Linux) and a documentation module. When you run the `.exe` file or the `.bin` file, make sure that the documentation module is in the same directory as the `.exe` file or the `.bin` file.

On Windows platforms, you can use an application such as Winzip to unzip the files.

On Linux platforms, run the following command to unzip the file:

```
unzip <filename>.zip
```

- 3 On Linux platforms, give the `.bin` file the execute permission.
- 4 Run the self-extracting file that is appropriate for your target platform. On Linux be sure that you are **not** logged on as *root*.

Create an ArcSight user to own the installation. Log in as the ArcSight user before running the Manager Installation Wizard.



#### About the ArcSight User

The ArcSight user can be whatever account name you want. However, this document cannot know what user name you used, so it refers to this user as user *arcsight*. If the text ever tells you to log in as user *arcsight*, it means to log in as the user that you created to run the ESM installation. That is the user who “owns” the installation.

The Manager installation file for each platform is described in the following table:

Platform	Installation File
Windows	<code>ArcSight-5.6.x.nnnn.y-Manager-Win64.exe</code>
Linux	<code>ArcSight-5.6.x.nnnn.y-Manager-Linux64.bin</code>

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

The Manager installation program provides a summary of the 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 track your progress. Click **Cancel** at any time, but the Manager is only usable if you complete the installation wizard successfully. 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 introduction and click **Next**.
- 2 Read the installation process checklist and click **Next**.

- 3 The “I accept the terms of the License Agreement” radio button is disabled until you scroll to the bottom of the agreement text. After you have read the License Agreement click the **I accept the terms of the License Agreement** radio button and click **Next**.



Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

- 4 Read the notice and click **Next**.
- 5 Enter or navigate to the location where you would like to install Manager and click **Next**.
- 6 Choose the location where you would like to create a shortcut for the Manager and click **Next**.
- 7 Review the summary in the Pre-Installation screen. If need be, click **Previous** to make any changes. When you are ready to proceed, click **Install**.

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

## Transferring Configuration from an Existing Installation

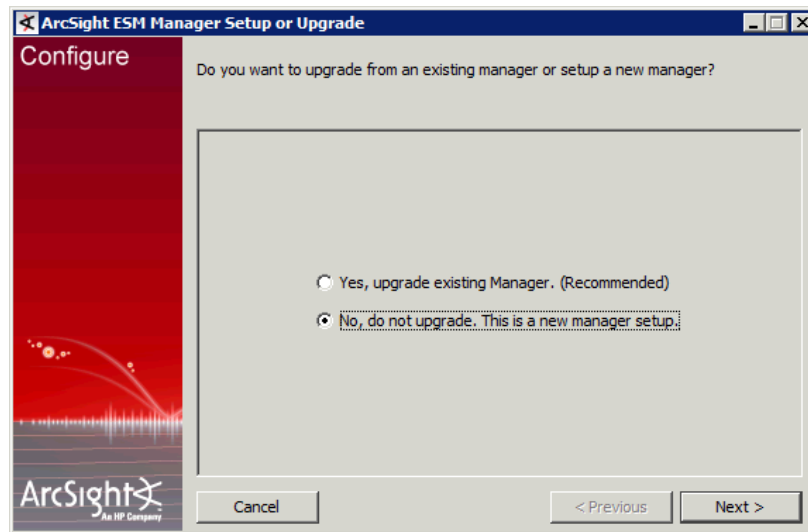
After the Manager has been installed, you see the first configuration screen.



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

The wizard asks if you would like to upgrade your existing Manager installation. Upgrading your Manager installation transfers configuration options from the previous installation of

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 Manager

Next, you see the following screen:



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

The default event hashing algorithm is SHA-256, which is a secure hash algorithm, that uses 32-byte (256 bits) words. It may be used by Federal agencies for applications using secure hash algorithms.

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

The 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.



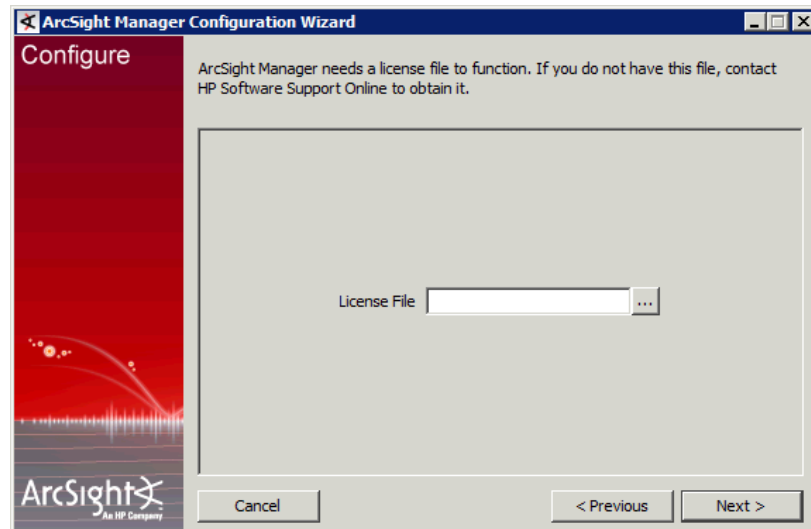
**Note**

You can re-configure 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 such as ArcSight Console) specify to talk to the 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).
Physical Location	Text describing the location of the Manager host machine.

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

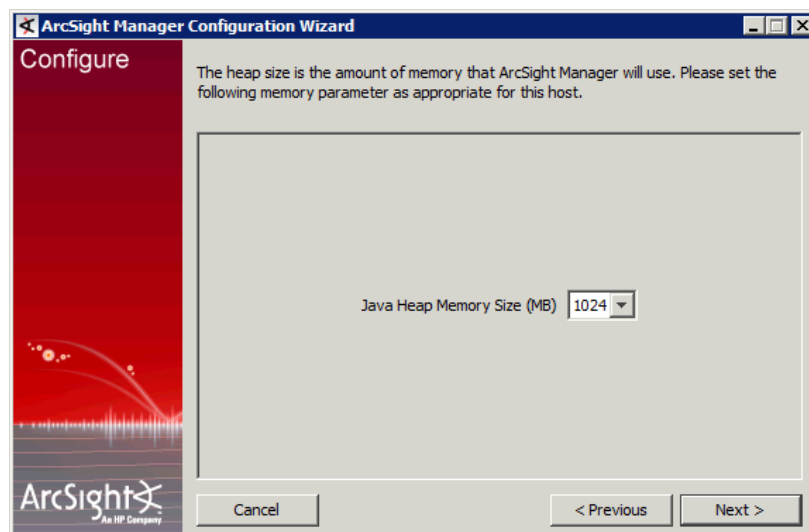
Enter the full path to the `arcsight.lic` file. The Configuration Wizard copies it to the appropriate folder.



Click **Next**.

## Java Heap Memory Size

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



The Java Heap memory size is the amount of memory that ESM allocates for its heap. (Besides the heap memory, the Manager uses some additional system memory as well.) The recommended size for production deployments is at least 1024 MB. (Smaller amounts 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 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

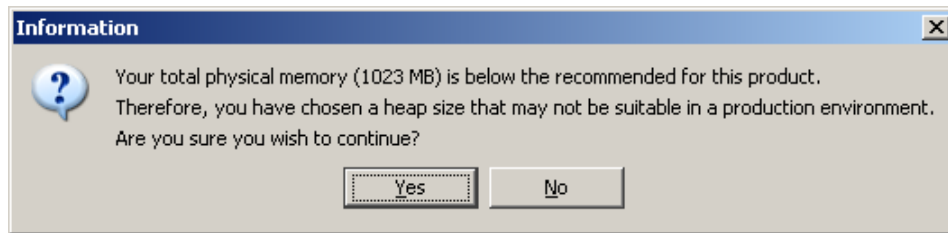
512 MB. If you specify a heap size of 1 GB, the system should have at least 1.5 GB of physical memory.



Supporting 50,000 actors requires an additional 2 GB of Java heap memory in the Manager. An additional 300 MB is needed for each category model you construct that uses 50,000 actors. This additional memory is not in use all the time, but is needed for certain operations.

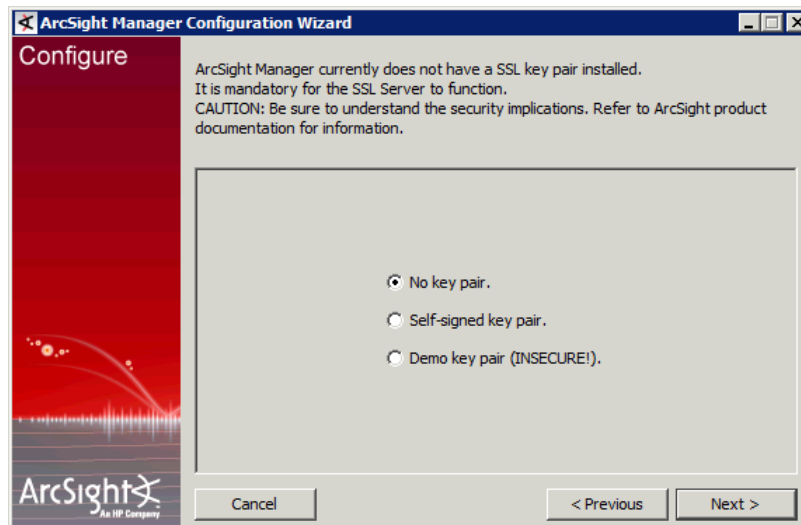
Set the memory parameter for the Manager host machine from the Java Heap Memory Size drop-down menu and click **Next**.

If your machine does not have sufficient memory for the Manager, you will see a message similar to the following:



## SSL Certification Selection

The Manager controls SSL certificate type for communications with the ArcSight Console, so the installer prompts you to select the type of SSL certificate that the Manager is to use.



## Deciding which SSL Certificate to Select

Manager should be installed with a self-signed or a Certificate Authority (CA) signed SSL certificate. Both are equally secure, however, CA-signed scales better. See ESM 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, we strongly recommend that you update it with a signed certificate as soon as possible for the following reasons:

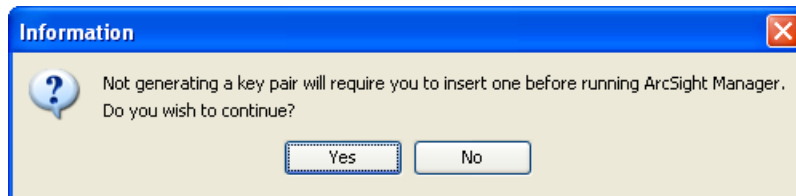
- Demo certificate is not secure. Systems running with this certificate can be easily compromised if attacked.
- When you replace the demo certificate with a signed certificate on the Manager, you have to update the certificate on all ArcSight Consoles, SmartConnectors, and ArcSight Web servers that 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 ESM components, see ESM Administrator's Guide.

## Selecting the SSL certificate

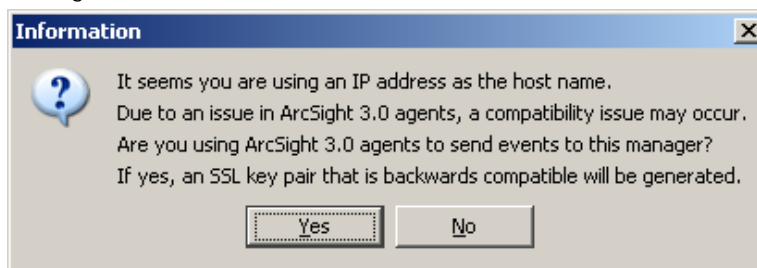
The Manager Configuration Wizard prompts you to specify the type of Secured Sockets Layer protocol (SSL) server certificate to use.

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



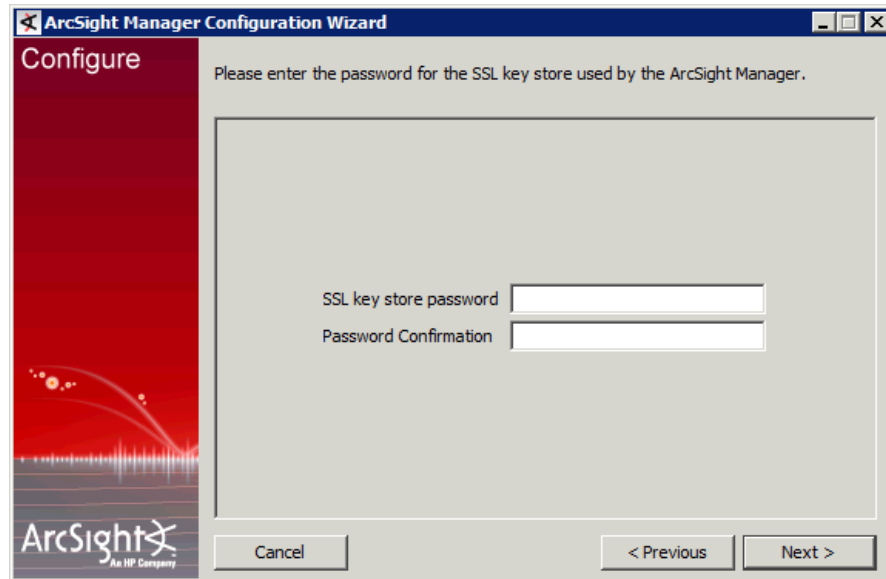
After completing the Configuration Wizard, follow the procedure described in ESM Administrator's Guide to install the CA-signed certificate.

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



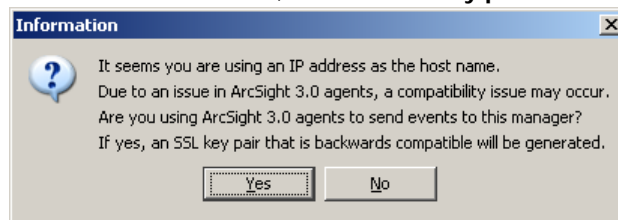
Enter the details of the certificate to be issued:

 A screenshot of the "ArcSight Manager Configuration Wizard" window, specifically the "Configure" step. The window has a dark blue title bar with the text "ArcSight Manager Configuration Wizard" and standard window controls. The main area has a light gray background. On the left, there is a red vertical banner with the ArcSight logo and the text "ArcSight An HP Company". The main content area contains the text "Please complete the following details about the SSL certificate to be issued." followed by a list of fields: "Validity (days)" with a value of "365", "Country", "State", "Locality", "Organization", and "Organizational Unit". At the bottom, there are three buttons: "Cancel", "< Previous", and "Next >".



Follow the procedure described in ESM 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. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration." Click **Next**:



After completing the Manager configuration, follow the procedure in ESM 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 Manager Configuration Wizard prompts you for the Oracle information that will be used to connect with an ArcSight Database.

The following table describes parameters 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 'ArcSight Manager Configuration Wizard' window with the 'Configure' tab selected. The text 'Please complete the following information about the database.' is displayed. The input fields are as follows:

- Oracle Host Name: [Empty text box]
- Oracle Port: [1521]
- Oracle SID: [arcsight]
- Database User Name: [Empty text box]
- Database Password: [Empty text box]

At the bottom, there 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 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 215](#) for details on setting up ESM to use a PKCS #11 token such as the Common Access Card (CAC).

---

By default, 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

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 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 Manager.

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

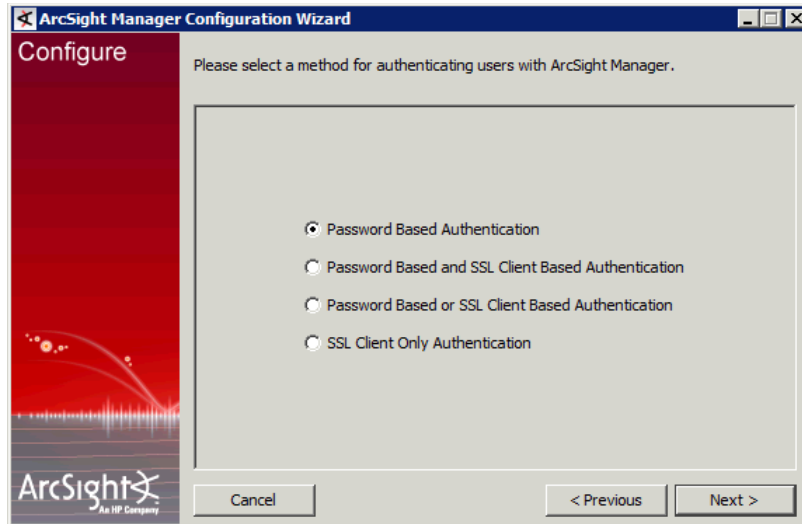
Once you select an external authentication mechanism, all user accounts, including the admin account, are authenticated through it.

## Guidelines for setting up external authentication

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

- All users who 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, 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.
- To impose restrictions on the information a user can access, set up Access Control Lists (ACLs) on the Manager.

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



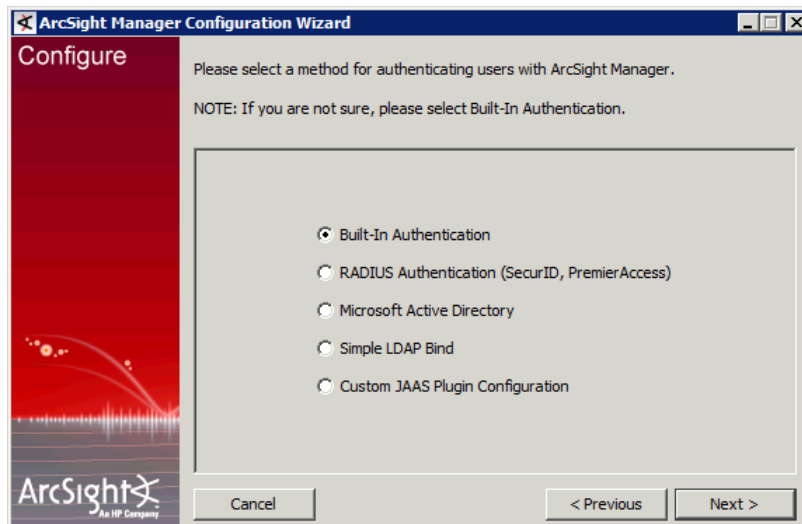
**Caution**

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 is based on the User name and Password that you enter when logging into the Console. If you select this option, you are 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 [“Manager Administrator Account Setup” on page 101](#) section.

## Setting up RADIUS Authentication

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

**ArcSight Manager Configuration Wizard**

**Configure**

Please fill out the following information about the RADIUS server.

Authentication Protocol: PAP

RADIUS Server Host:

RADIUS Server Type: RSA Authentication Manager

RADIUS Server Port: 1812

RADIUS Shared Secret:

Buttons: Cancel, < Previous, 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. 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"> <li>• RSA Authentication Manager</li> <li>• Generic RADIUS Server</li> <li>• Safeword PremierAccess</li> </ul>
RADIUS Server Port	Specify the port on which the RADIUS server is running.
RADIUS Shared Secret	Specify the RADIUS shared secret string used to verify the authenticity and integrity of the messages exchanged between the Manager and the RADIUS server.

The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo and the text 'An HP Company'. 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, there are two text input fields: 'User Name' and 'User Password'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The ArcSight logo is also present in the bottom left corner of the main area.

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

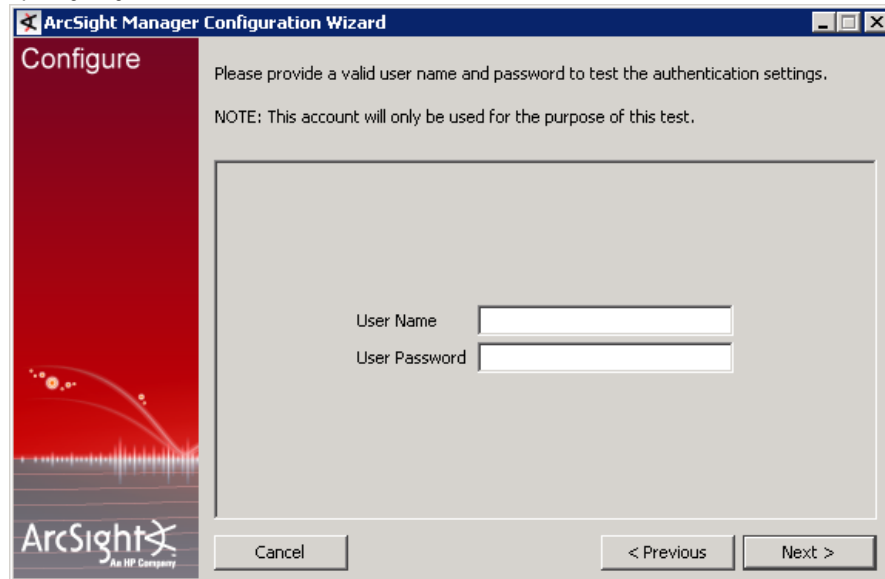
### Setting up Active Directory User Authentication

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.

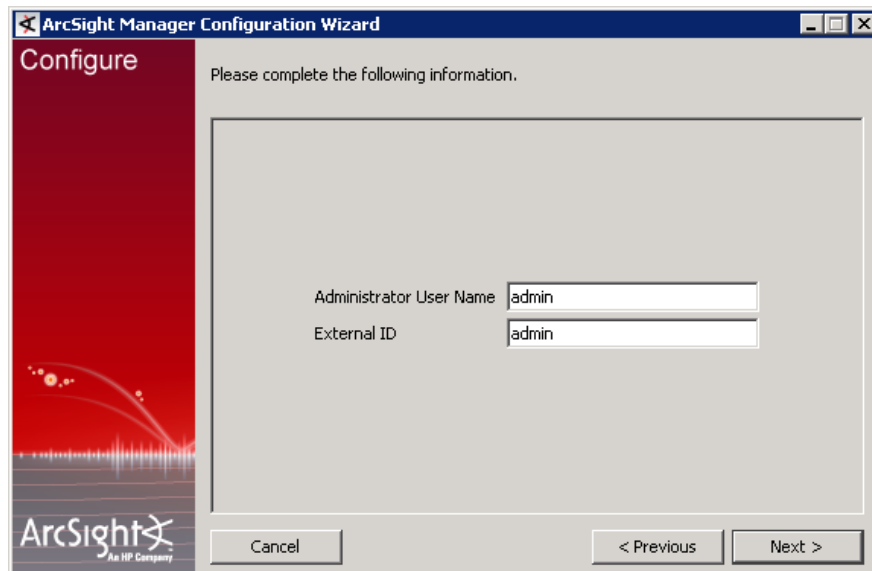
Parameter	Description
Active Directory Server	Host name of the Active Directory Server.
Enable SSL	<p>Whether the Active Directory Server is using SSL. The default is True (SSL enabled on the AD server).</p> <p>No further SSL configuration is required for the AD server.</p> <p>Whether you selected SSL earlier for communications with the Console is irrelevant. Certificate type is set on the AD server side, not the manager.</p>
Active Directory Port	Specify the port to use for the Active Directory Server. If the AD server is using SSL (Enable SSL=true), use port 636. If SSL is not enabled on the AD server, use port 389.
Search Base	Search base of the Active Directory domain; for example, DC=company, DC=com.
User DN	<p>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.</p> <p>The CN of the user is the "Full Name," not the user name.</p> <p><b>Note:</b> If your domain name contains a backslash (\), use a double backslash (\\) instead.</p>
Password	Domain password of the user specified earlier.
Allowed User Groups	Comma-separated list of Active Directory group names. Make sure that the commas are not followed by a space, for example testgroup1,testgroup2. Only users belonging to the groups listed here will be allowed to log in.

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



The screenshot shows the 'Configure' step of the ArcSight Manager Configuration Wizard. The window title is 'ArcSight Manager Configuration Wizard'. The left sidebar has a red background with the ArcSight logo and 'An HP Company' text. 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, there are two text input fields: 'User Name' and 'User Password'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

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



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

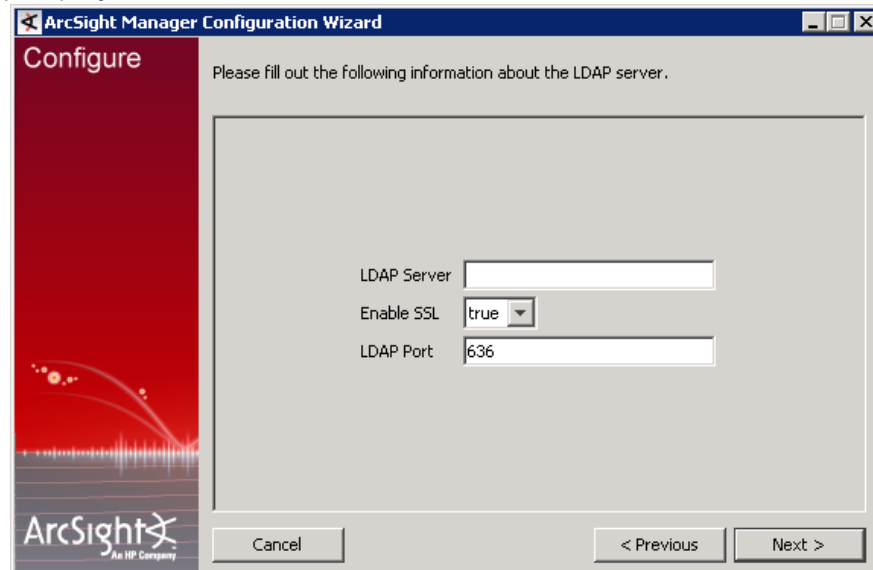
### Configuring AD SSL

If you are using SSL between the Manager and your authentication server, you must ensure that the server's certificate is trusted in the Manager's trust store

<ARCSIGHT\_HOME>\jre\lib\security\cacerts, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in ESM Administrator's Guide.

## Setting up LDAP Authentication

The 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 image shows a screenshot of the 'ArcSight Manager Configuration Wizard' window, specifically the 'Configure' step. The window has a red sidebar on the left with the ArcSight logo and the text 'An HP Company'. The main area is titled 'Please fill out the following information about the LDAP server.' and contains three input fields: 'LDAP Server' (a text box), 'Enable SSL' (a dropdown menu currently set to 'true'), and 'LDAP Port' (a text box containing '636'). At the bottom of the window are three buttons: 'Cancel', '< Previous', and 'Next >'.

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

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



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 and 'An HP Company' text. 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 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.

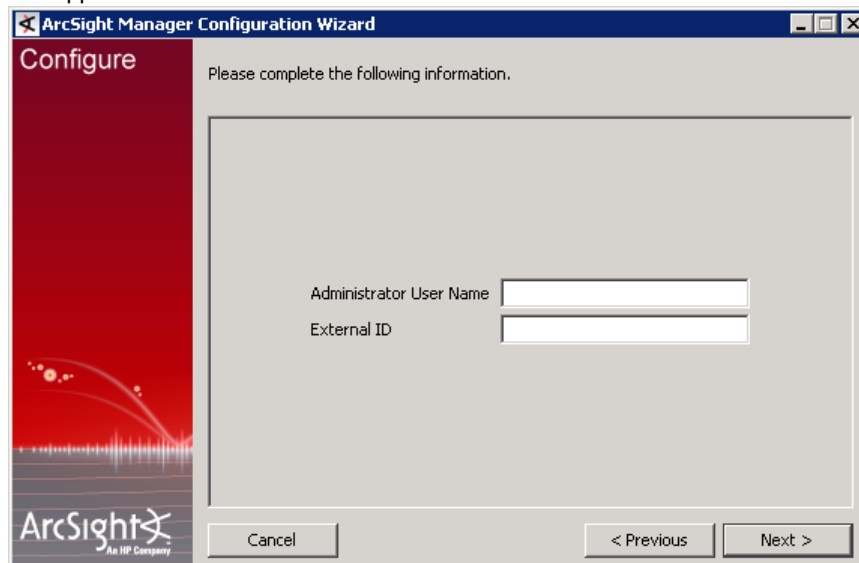


**Note**

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.

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



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 and 'An HP Company' text. 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' and 'External ID'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

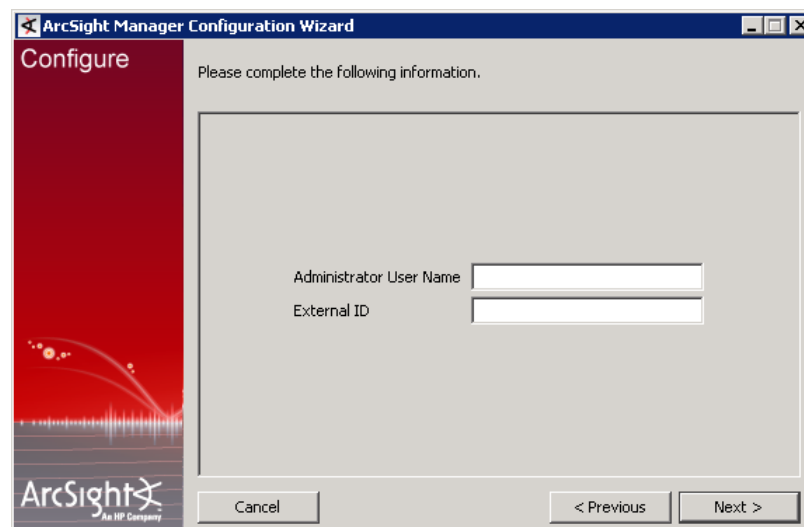
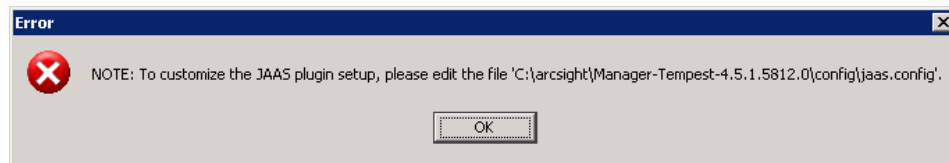
### Configuring LDAP SSL

If you are using SSL between the Manager and your authentication server, ensure that the server's certificate is trusted in the Manager's trust store

<ARCSIGHT\_HOME>\jre\lib\security\cacerts, whether the authentication server is using self-signed or CA certificates. For CA certificates, if the Certificate Authority (CA) that signed your server's certificate is already listed in cacerts, you do not need to do anything. Otherwise, obtain a root certificate from the CA and import it in your Manager's cacerts using the keytoolgui utility. For more information on importing certificates, see Understanding SSL Authentication in ESM Administrator's Guide.

### 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 Manager `config` directory.



### Password Based and SSL Client Based Authentication

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



Note

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

Manually set up the authentication of the client certificate by the Manager. See the 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.

## 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"> <li>• The CN name used by your PKCS#11 token</li> <li>• Name in the client based SSL certificate</li> <li>• Radius username</li> <li>• Active Directory Login name</li> <li>• LDAP Login name</li> </ul>
Administrator Password	Administrator's password
Password Confirmation	Re-enter the password to confirm

For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration," "Managing Password Configuration," "password Character Sets."

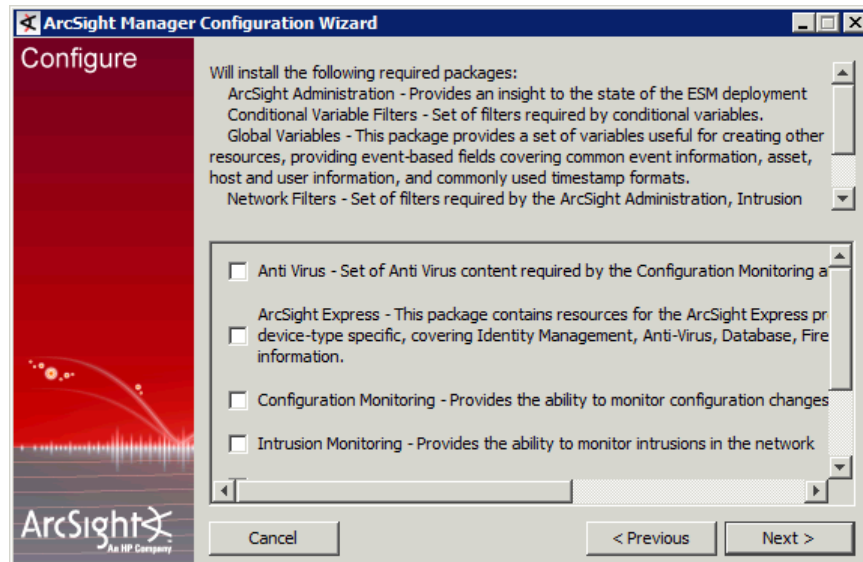
The Administrator user name and password are the user name and password that you will use when you first log in to the ArcSight Console. Using the ArcSight Console, you can add additional administrators by adding users to the Administrator's group.

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

## Select Packages

The System Content is now delivered in the form of packages. System content packages are automatically installed as a part of 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 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 above) and need not be installed separately.

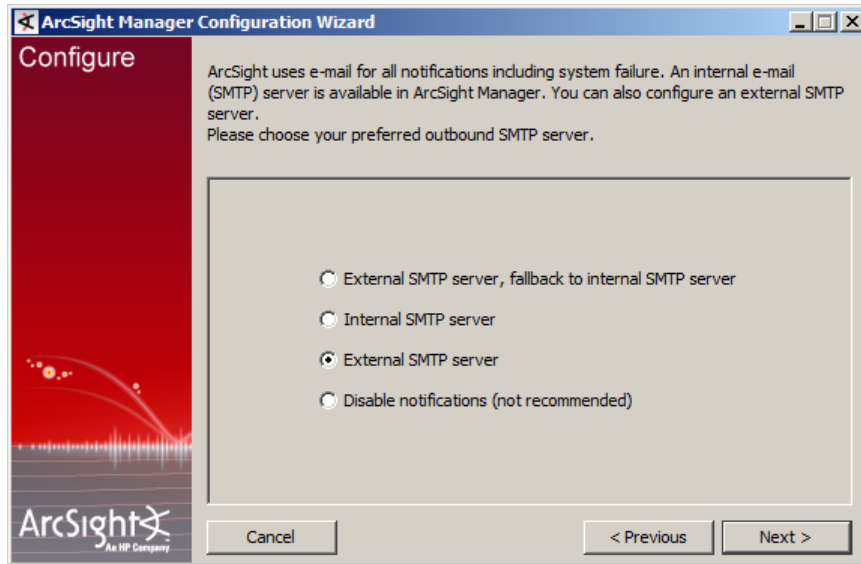
For more information about packages, see the ESM System Content Guide.

## Mail Server



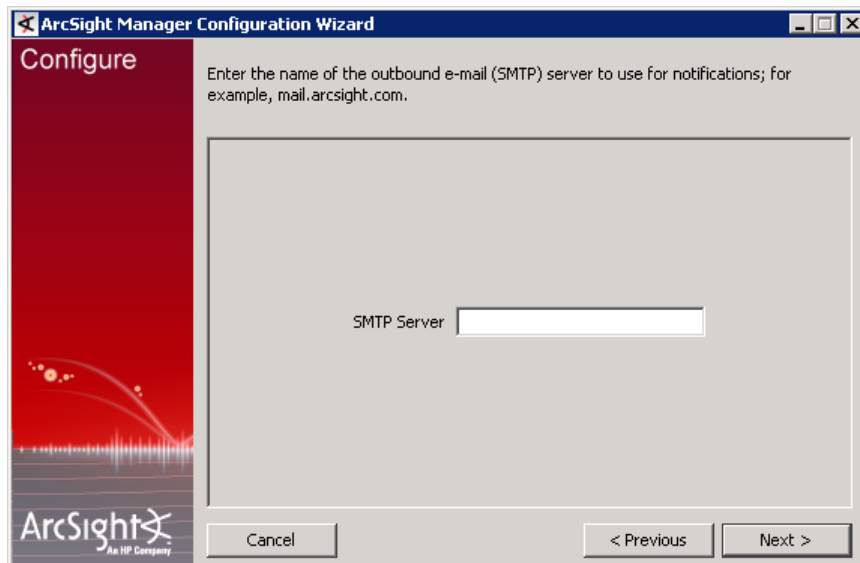
Set up notification and specify notification recipients in order to receive system warnings. The importance of this step is sometimes overlooked, leading to preventable system failures.

You will be prompted to select a SMTP server:

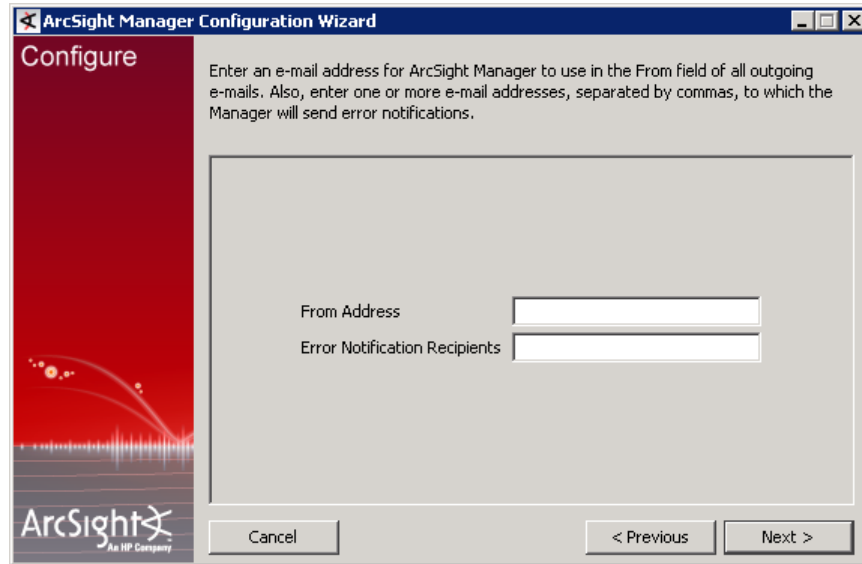


HP ArcSight recommends that you configure the external SMTP server.

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



You are then 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 and 'An HP Company' text. The main area has a light gray background. At the top, it says 'Configure' in red. Below that, a text box explains: '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.' There are two text input fields: 'From Address' and 'Error Notification Recipients'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The ArcSight logo is also at the bottom left of the main area.

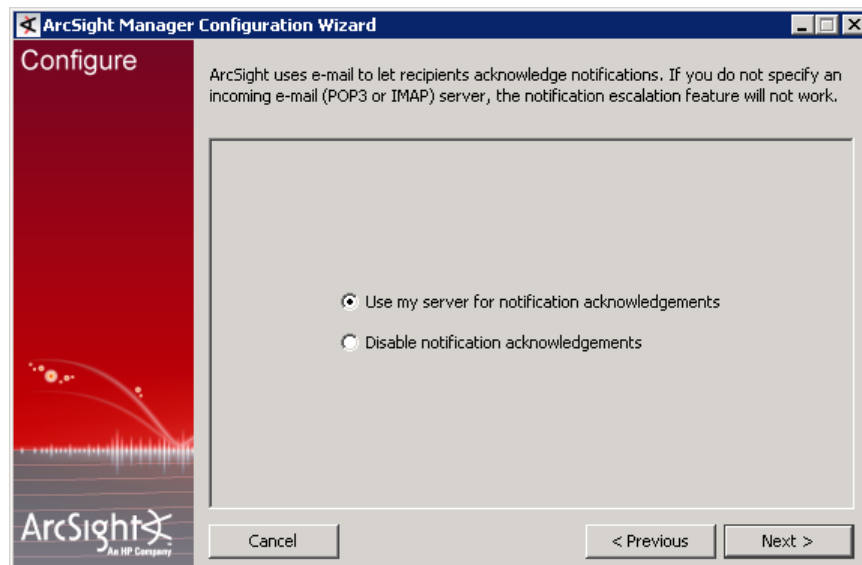
**Configure**

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 and 'An HP Company' text. The main area has a light gray background. At the top, it says 'Configure' in red. Below that, a text box explains: '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.' There are two radio button options: 'Use my server for notification acknowledgements' (which is selected) and 'Disable notification acknowledgements'. At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The ArcSight logo is also at the bottom left of the main area.

**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 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 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 Manager will use to receive notification confirmations
Server Protocol	Either the IMAP or POP3 protocol used by the Manager to communicate with the Incoming Mail Server
User Name	The username that the Manager will use to login to the Incoming Mail Server
Password	The password that the Manager will use to login to the Incoming Mail Server

Configure the Outgoing Mail Server to accept and relay e-mail sent from the From Address e-mail address.

## ArcSight Web



Note

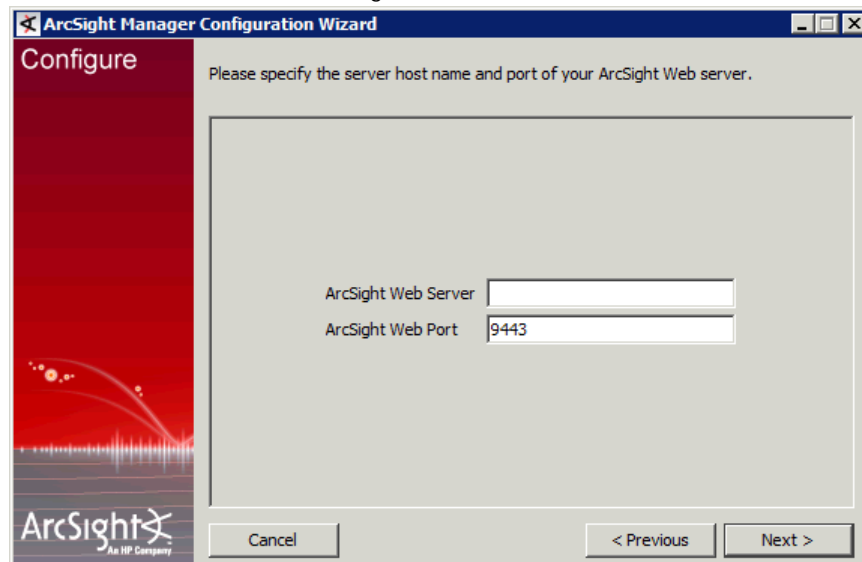
If you choose not to enter a URL for the ArcSight Web at this point, you can do so any time later by issuing the following command from

<ARCSIGHT\_HOME>\bin directory:

```
arcsight managersetup
```

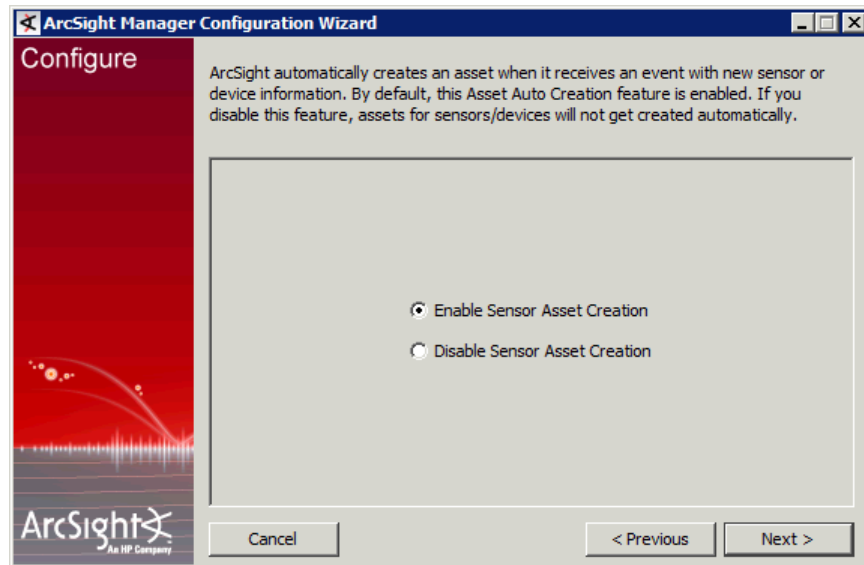


If you chose the **Enter URL for ArcSight Web to view reports/events** option, enter the information for the ArcSight Web server:



## Asset Auto Creation

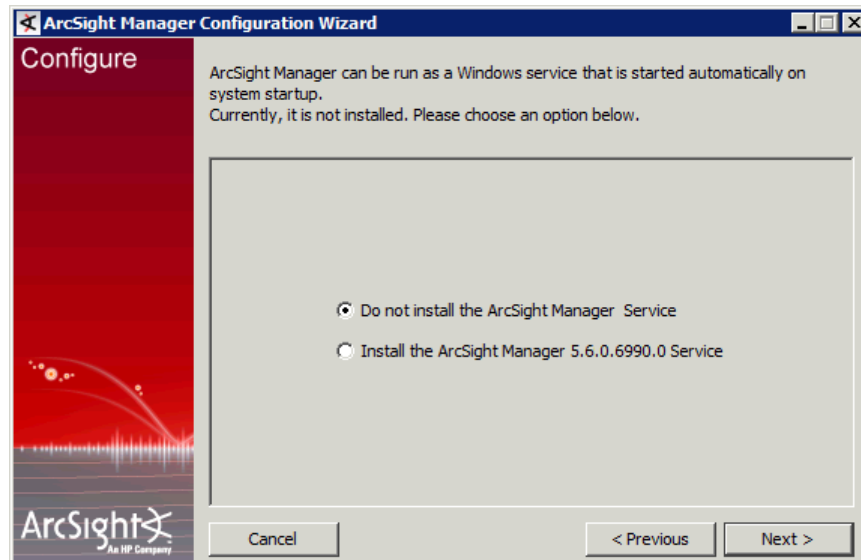
Manager can automatically create an asset when it receives an event with a new sensor or device information. By default, assets are automatically created. If you want to disable this feature, select **Disable Sensor Asset Creation**.



## Setting up as a Service or Daemon

The Configuration Wizard next offers to set up 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.

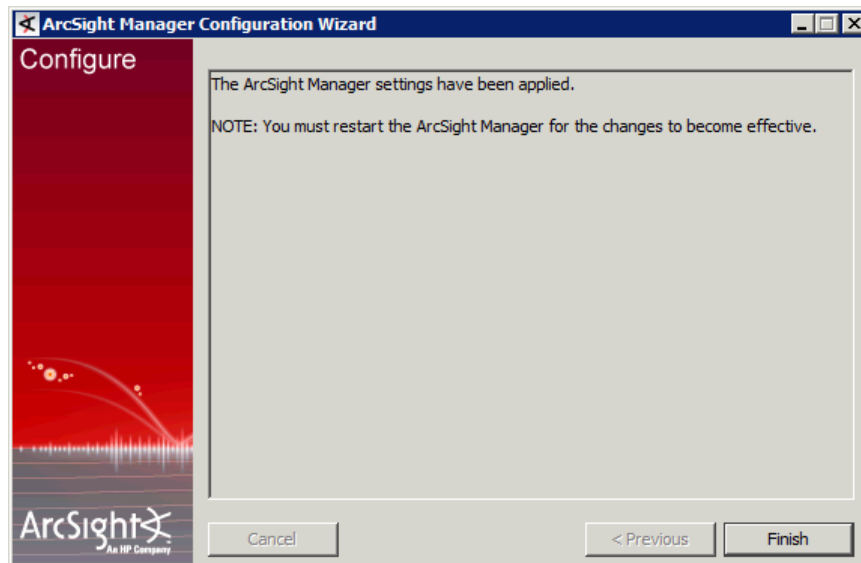
Choose whether you want to install the Manager as a service, then click **Next**.



If you choose the option to install Manager as a service, the installer prompts you to specify parameters used to set up the service. If you choose not to install Manager as a service, you can change the startup configuration later. For more information, see [“Running the Manager as a Service” on page 109](#).

The Configuration Wizard returns a message indicating the Manager configuration is ready to be applied. Click **Next**.

After Manager settings have been applied, click **Finish**.



After installation is complete, you get a message saying that the Manager has been installed successfully. Click **Done**.

You can start the Manager now.



**Note**

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

On Linux 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.

## Starting and Stopping the Manager

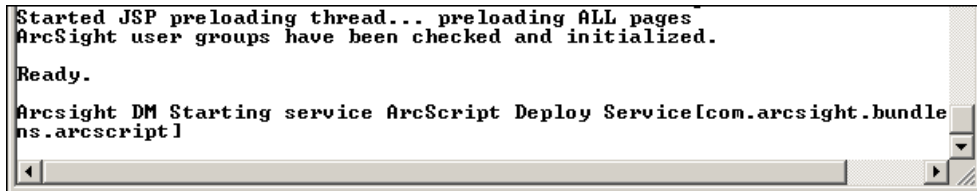
### Starting the Manager

To start 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 Manager's `<ARCSIGHT_HOME>\bin` directory:
- 3 Type in the following line and press **Enter**:

```
arcsight manager
```

When the Manager starts up, it 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.



```
Started JSP preloading thread... preloading ALL pages
ArcSight user groups have been checked and initialized.
Ready.
Arcsight DM Starting service ArcScript Deploy Service[com.arcsight.bundle
ns.arcsriptl
```

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 Manager, open a separate command prompt window and issue the following command:

```
arcsight managerstop
```

## Running the Manager as a Service



Note

### Platform-specific notes:

**On Windows**, when you start the Manager as a service, the Manager status update timeout is smaller than the time the Manager takes to start, resulting in the service timing out before the Manager is started. To avoid receiving this error message, you can configure the overall Windows system's service startup timeout by following the procedure in <http://support.microsoft.com/kb/824344>.

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

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

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

Script output goes to `<ARCSIGHT_HOME>/logs/default/server.script.log`. The `stdout` output of the Manager goes 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

When you start the Manager, the command window shows a running display of Manager activities. Watch for the word "Ready" when it has fully initialized and is ready to respond to communications. The ready status is also recorded in the `server.std` log.

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

## Reconfiguring Manager

To reconfigure Manager settings made during installation, shutdown the Manager and then run the 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 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. ESM'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`.



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

---

## Securing the Manager Properties File

The 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 Manager. As a result, the `server.properties` file must be protected so that only the user account under which the Manager is running is able to read it. This can be accomplished as follows:

### On Linux platforms:

Run:

```
chmod 600 server.properties
```

### On Windows:

- 1 As Windows administrator, go to the Manager's `config` directory.
- 2 Right-click the `server.properties` file, and choose **Properties** to open the Properties dialog.
- 3 Click the **Security** tab then click **Advanced**.
- 4 In the Advanced Security Settings dialog for the file, select **Users** and uncheck the box that says "Allow inheritable permissions from the parent to propagate to this object and all child objects...".

- 5 At the prompt that appears, click **Copy**.
- 6 Click **Apply** on the Advanced Security Settings dialog. Then click **OK**.
- 7 On the Properties dialog, select the **Users** group and click **Remove**.
- 8 Select the **SYSTEM** group and click **Remove**.
- 9 Click **Apply** then click **OK**.

Now you should only see Administrators listed in the **Security** tab.

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

## Sending Events as SNMP Traps

ESM 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). ESM'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 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 are 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 depends 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 SmartConnector SDK format. All ESM 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:

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

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

ESM 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 Manager

Stop Manager before uninstalling it.

To uninstall on Windows, run the **Start->All Programs ->ArcSight Manager ->Uninstall ArcSight Manager 5.6** program. 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 Linux 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 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 F, Installing ESM in FIPS Mode, on page 171](#). Section [“Differences Between Default and FIPS Modes” on page 21](#) lists the basic differences between the three modes.

The following topics are covered in this chapter:

- [“Console Supported Platforms” on page 115](#)
- [“Using a PKCS#11 Token” on page 115](#)
- [“Installing the Console” on page 116](#)
- [“Starting the ArcSight Console” on page 125](#)
- [“Reconnecting to the ArcSight Manager” on page 127](#)
- [“Reconfiguring the ArcSight Console” on page 127](#)
- [“Uninstalling the ArcSight Console” on page 128](#)

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. Typically, ArcSight Console is deployed on several perimeter machines located outside the firewall which protects the ArcSight Manager and Database hosts.

## Console Supported Platforms

Refer to the Product Lifecycle document available on the Protect 724 website for the most current information on supported platforms.

## Using a PKCS#11 Token

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 215](#) for details on using a PKCS #11 token with the Console.

## Installing the Console



Caution

On Macintosh platforms, please make sure that:

- You are using an intel processor based system
- You have the JRE installed on your system before installing the Console. Refer to the Release Notes for the version of JRE to install
- 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 Linux based system, you will notice a few Linux-specific screens. Path separators are / for Linux and \ for Windows.



Note

On Macintosh platform:

- If your JRE gets updated, you will see the following error when you try to log into the Console:

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

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

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

- Before you start the Console, make sure to set up a default printer to which to print. if you open a channel, select some rows, right-click on them and select **Print Selected Rows** from the resulting menu, the Console will crash if a default printer is not set up.

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

- 1 Download the ESM installation file appropriate for your platform from the HP SSO Download site (ArcSight-5.6.x.nnnn.y-Console-<platform>.zip). Copy all the files (without extracting their contents) to a temporary directory.



Caution

Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party. Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

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

Platform	Installation File
Linux	ArcSight-5.6.x.nnnn.y-Console-Linux.bin
Windows	ArcSight-5.6.x.nnnn.y-Console-Win.exe
Macintosh	ArcSight-5.6.x.nnnn.y-Console-MacOSX.zip

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



**Caution**

You can use spaces in the path name for the ArcSight Console installation in Windows *only*.

Other than that, make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms with the exception of spaces for the ArcSight Console install on Windows.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

- 6 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.

- 7 Select where you would like to create a shortcut for the Console and click **Next**.
- 8 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.

## Character Set Encoding

Install the Console on a machine that uses the same character set encoding as the Manager.

If the character encodings do not match, then user IDs and passwords are restricted to using the following characters:

a-z A-Z 0-9 \_@. # \$ % ^ & \* + ? < > . { } | , ( ) - [ ]

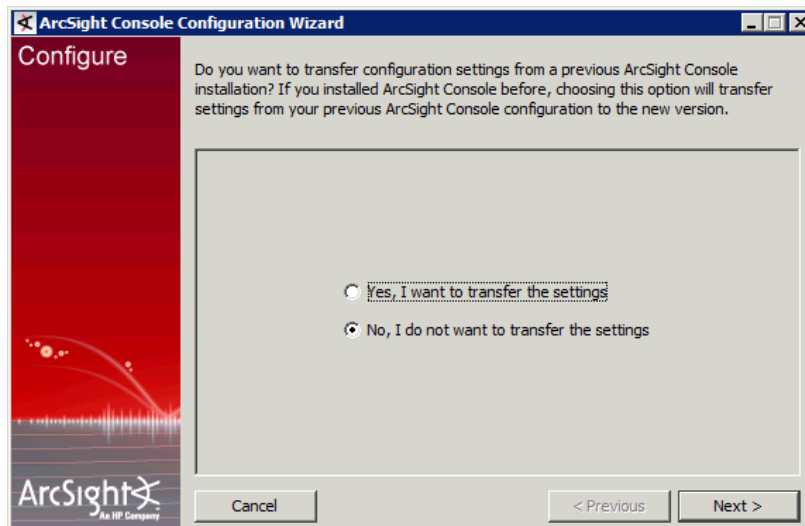
If the Console encoding does not match and a **user ID** contains other characters, That user should not save any custom shortcut key (hot key) schema. The user ID is not properly encoded in the keymap .xml file and that makes it impossible to establish the user's shortcut schema during login. In that circumstance, *all logins fail* on that Console.

If you must use a non-UTF-8 encoding, and you must have user IDs with other characters in them then custom shortcut keys are not supported on any Console where these users would log in. In that situation add the following property to the console.properties file: console.ui.enable.shortcut.schema.persist=false. This property prevents custom shortcut key schema changes or additions.

If the Console encoding does not match and a **password** contains other characters, that user cannot log in from that Console, as the password hash won't match the one created on the Manager when the password was created.

## Transferring Configuration from an Existing Installation

After the Console has been installed, the wizard asks if you would like to transfer configuration options from an existing installation of ArcSight Console. Choose **No, I do not want to transfer the settings** to create a new, clean installation and click **Next**.



## 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**.

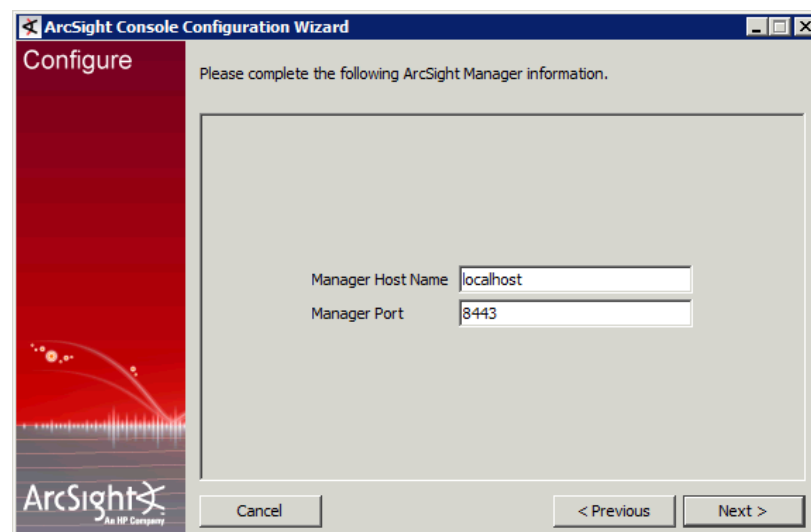
## Manager Connection

The ArcSight Console configuration wizard prompts you to specify the ArcSight Manager with which to connect. Enter the host name of the Manager to which the Console will connect.

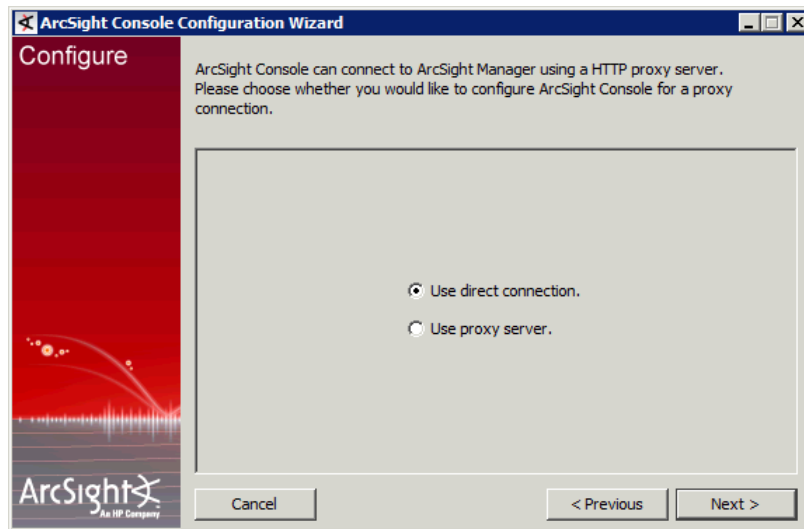


Do not change the Manager's port number.

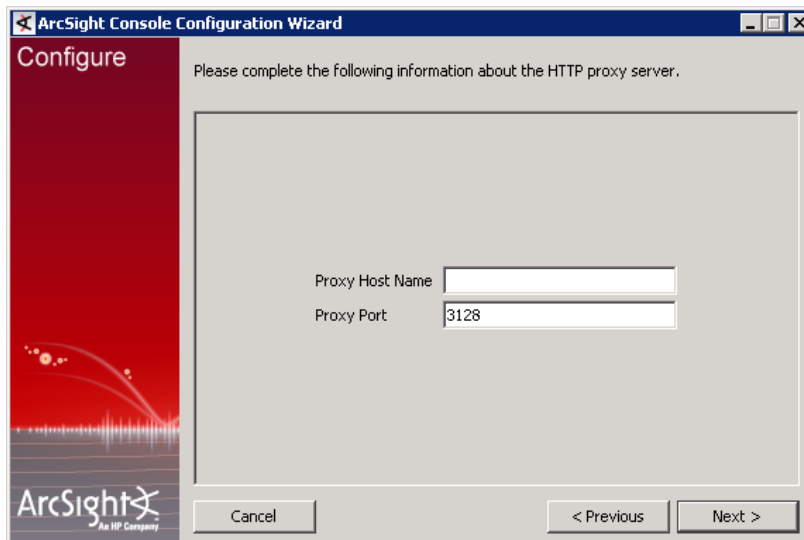
Click **Next**.



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



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



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

## Authentication



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

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

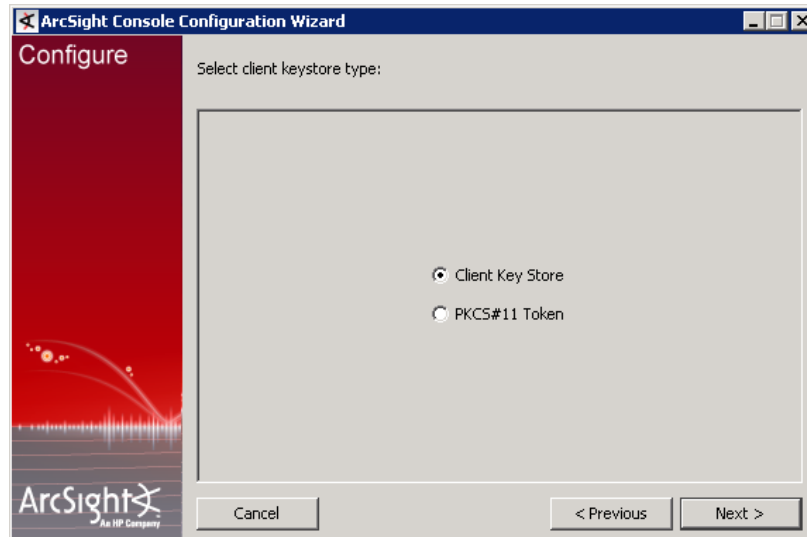


**Password Based and SSL Client Based Authentication** option currently supports only client keystore for SSL based authentication. Using PKCS#11 token as your SSL Client Based authentication method within the **Password Based and SSL Client Based Authentication** option is not currently supported.

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

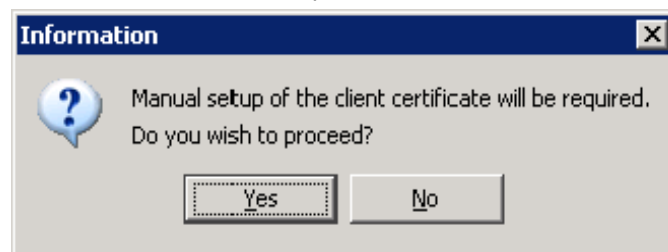
If you select **Password Based and SSL Client Based Authentication**, you will be required to enter both user name/password combination and you will be required to setup your client certificate manually. Follow the procedure described in ESM Administrator's Guide to set up the client certificate.

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 215](#) 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.

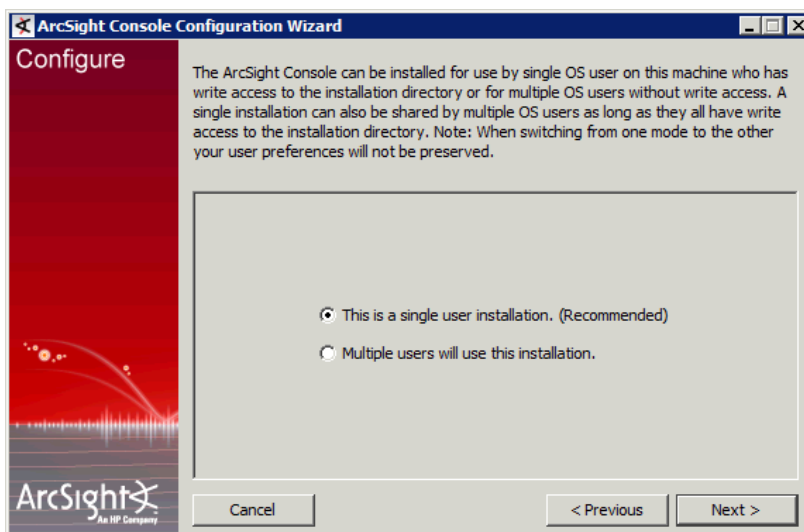
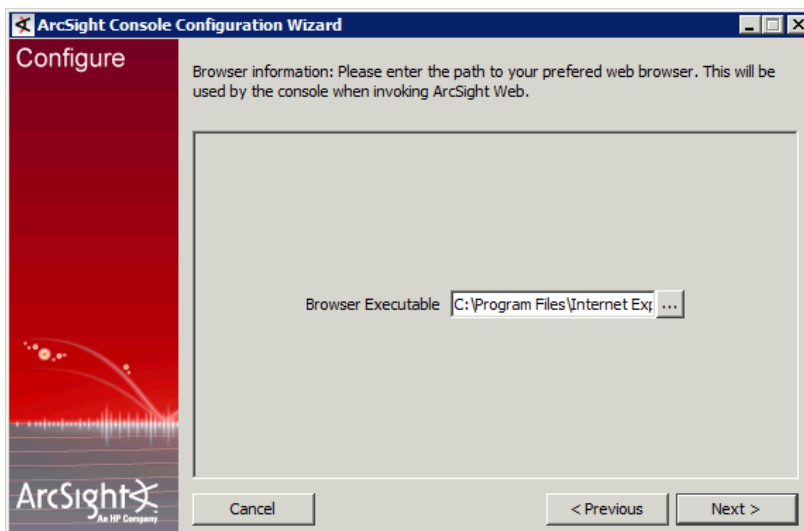


After completing the Configuration Wizard, follow the procedure described in ESM Administrator's Guide to set up the client certificate.

## Web Browser

The ArcSight Console configuration wizard prompts you to specify the default web browser you want to use to display reports, Knowledge Centered Support 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 Centered Support articles and other web pages launched from the ArcSight Console. 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`

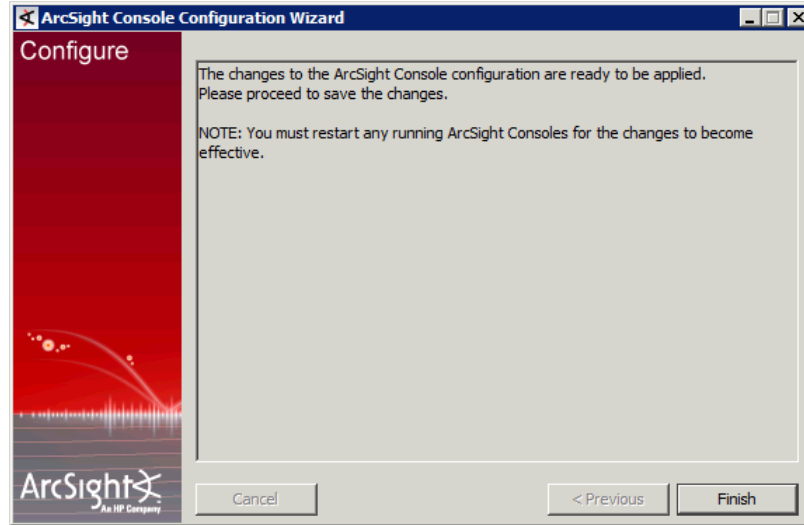
All other commands require write permission to the Console's `\current` directory.



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.



**Note**

#### On Mac OS X 10.5 update 8 and later:

The Mac OS update changed the password for the cacerts file in the system's JRE. Before you start the Console, you need to change the default password for the cacerts file by setting it to the following in the `client.properties` file (create the file if it does not exist) in the Console's `\current\config` folder by adding:

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

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



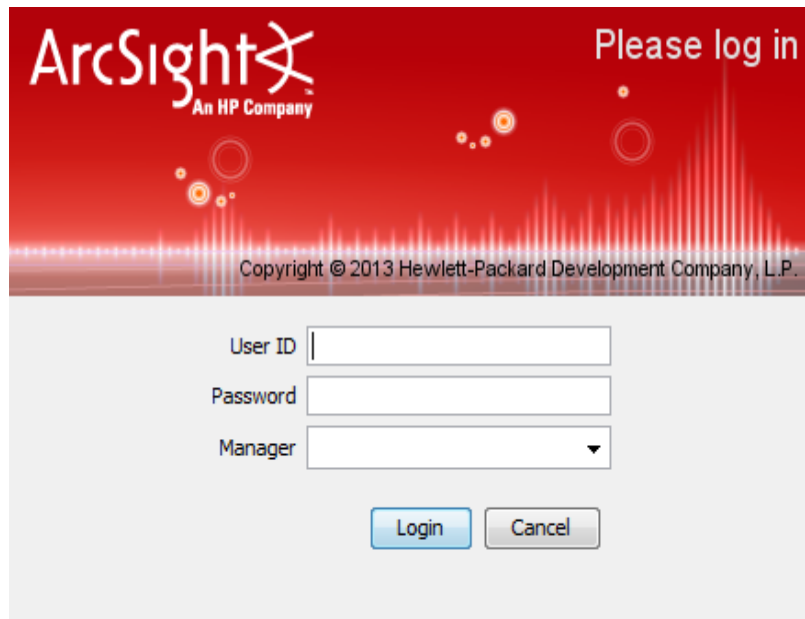
**Note**

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"> <li>• Login (username and password)</li> <li>• SSL Client Login</li> <li>• Cancel</li> </ul> If you selected PKCS#11 Token, you will see <ul style="list-style-type: none"> <li>• PKCS #11 Login</li> <li>• Login</li> <li>• Cancel</li> </ul>
SSL Client Only Authentication	If you selected Client Keystore as your authentication method, you will see <ul style="list-style-type: none"> <li>• Login (username and password)</li> <li>• Cancel</li> </ul> If you selected PKCS #11 Token, you will see <ul style="list-style-type: none"> <li>• PKCS #11 Login (SSL client authentication)</li> <li>• Cancel</li> </ul>

## Logging into the Console

To start the Console, click **Login**. When you start the Console for the first time, after you click Login, you will get a dialog asking you whether you want to trust the Manager's certificate. The prompt will show details specific to your settings (following is just an example). Click **OK** to trust the Manager's certificate. The certificate will be permanently stored in the Console's truststore and you will not see the prompt again the next time you log in.



## Reconnecting to the ArcSight Manager

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

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

## Reconfiguring the ArcSight Console

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

```
arcsight consolesetup
```

and follow the prompts.

## Turn Off Database Recycle Bin

After completing a new installation, you may see an error message in the Console. To work around it, turn the database recyclebin parameter off. Use the following commands:

```
prompt > arcdbutil sql
SQL>conn / as sysdba
SQL>ALTER SYSTEM set recyclebin=off scope=spfile;
SQL>shutdown immediate;
SQL>startup
SQL> show parameter recyclebin
SQL>exit
```

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

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

## Uninstalling the ArcSight Console

Before uninstalling the ArcSight Console, exit the current session.

To uninstall on Windows, run the **Start->All Programs->ArcSight Console ->Uninstall ArcSight Console 5.6**

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

```
Uninstall_ArcSight_Console.exe
```

To uninstall on Linux hosts, open a command window on the <ARCSIGHT\_HOME>/UninstallerData directory and run the command:

```
./Uninstall_ArcSight_Console
```



The UninstallerData directory contains a file `.com.zerog.registry.xml` with Read, Write, and Execute permissions for everyone. On Windows hosts, these permissions are required for the uninstaller to work. However, on Linux 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 F, Installing ESM in FIPS Mode, on page 171](#). To install the Web in FIPS with Suite B mode, see [Appendix G, Installing ESM in FIPS with Suite B Mode, on page 201](#). Section “Differences Between Default and FIPS Modes” on page 21 lists the basic differences between the three modes.



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 130
- “Starting ArcSight Web Manually” on page 139
- “Connecting to ArcSight Web” on page 139
- “Styling ArcSight Web” on page 140
- “Uninstalling ArcSight Web” on page 140

## ArcSight Web Supported Platforms

The list of supported platforms for ArcSight Web v5.6 is same as the one for ArcSight Manager v5.6.



- On 64-bit machines a minimum of 4 GB RAM is required.
- Refer to the ArcSight ESM Product Lifecycle document available on the Protect 724 site for the most current information on supported platforms.

## 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. Refer to the Product Lifecycle document available on the Protect 724 website for the most current information on supported browsers.

## Using a PKCS#11 Token

**Note**

- PKCS #11 token support may not be available for all ESM versions and ArcSight Express models.
- For this release, the use of PKCS#11 token is supported on Windows XP platform only.

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 215](#) for details on using a PKCS #11 token with ArcSight Web.

## Installing ArcSight Web

**Note**

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

- 1 Download the ESM installation file appropriate for your platform from the HP SSO Download site `ArcSight-5.6.x.nnnn.y-Web-<platform>.zip`. Copy all the files (without extracting their contents) to a temporary directory.

**Caution**

Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party. Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

- 2 Extract the installation files from the compressed file.



- Installing ArcSight Manager also requires you to extract its installation files from a compressed file. Installation files for ArcSight Web and ArcSight Manager should be **not** be present in the same folder. So, make sure that you do **not** extract the ArcSight Web files into the folder where you have extracted the ArcSight Manager files.
- After unzipping, you will see a .exe file (on Windows) or a .bin file (on Linux) and a documentation module. When you run the .exe file or the .bin file, make sure that the documentation module is in the same directory as the .exe file or the .bin file.

On Windows platforms, you can use an application such as Winzip to unzip the files.

On Linux platforms, run the following command to unzip the file:

```
unzip <filename>.zip
```

- 3 On Linux platforms, give the .bin file the execute permission.
- 4 Run the self-extracting file that is appropriate for your target platform. On Linux be sure that you are **not** logged on as root.

The following table lists all the installation files:

Platform	Installation File
Windows	ArcSight-5.6.x.nnnn.y-Web-Win.exe
Linux	ArcSight-5.6.x.nnnn.y-Web-Linux.bin

- 1 Read the introduction and click **Next**.
- 2 Read the installation process checklist and click **Next**.
- 3 The "I accept the terms of the License Agreement" radio button will be disabled until you read and scroll to the bottom of the agreement text. After you have read the License Agreement click the **I accept the terms of the License Agreement** radio button and click **Next**.
- 4 Read the notice and click **Next**.



Make sure that the path containing the installation file does not have any spaces or other special characters (just letters and numbers) in any of the folder names. These special characters are not supported in install paths for ESM components. If you have any of these characters in the install path, the ESM setup wizards might not work, and ESM Manager startup generates exceptions. This is an issue on all platforms.

If you modify the default install path, make sure there are no spaces or any other special characters in the directory names.

- 5 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**.

- 6 Choose a location where you would like to create a shortcut for ArcSight Web and click **Next**.
- 7 View the summary in the Pre-Installation Summary screen and click **Install** if you are satisfied with the paths listed. If you want to make any changes, use the Previous button to do so.

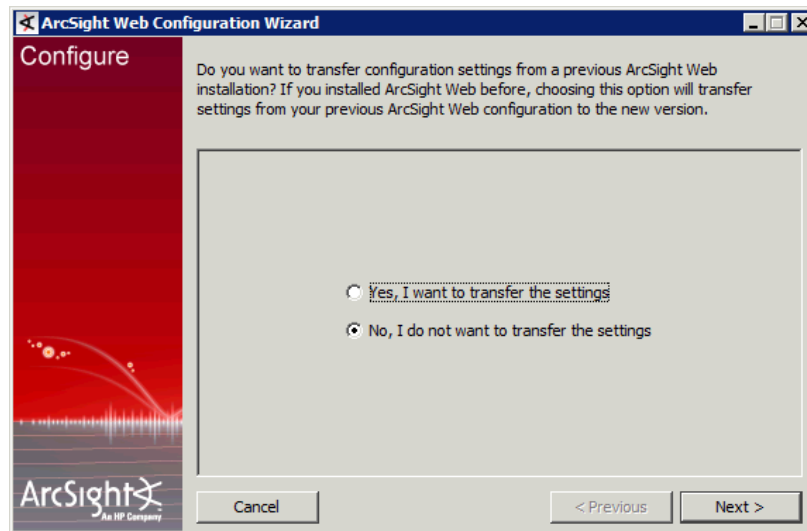
You can monitor the installation progress in the next screen.

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

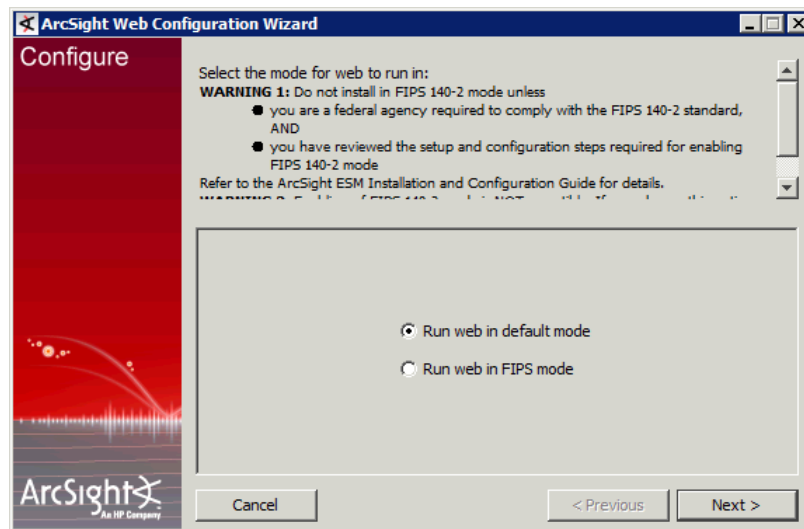
If you would like to set up SSL client authentication, you will need to replace the `cacerts` file in your ArcSight Web's `<ARCSIGHT_HOME>\jre\lib\security` with the `cacerts` file from your Manager's `<ARCSIGHT_HOME>\jre\lib\security` folder **before** you configure ArcSight Web. Follow the steps in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



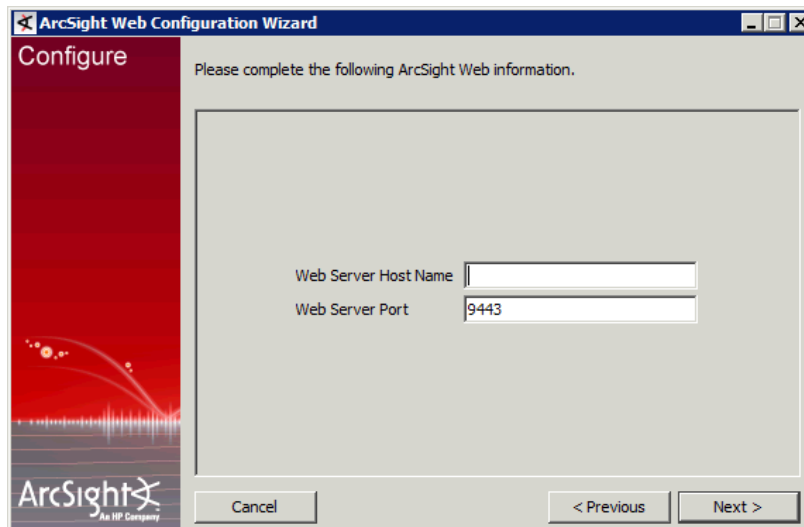
Keep in mind that once you have made your choice and clicked Next, you can not revert to this screen.



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

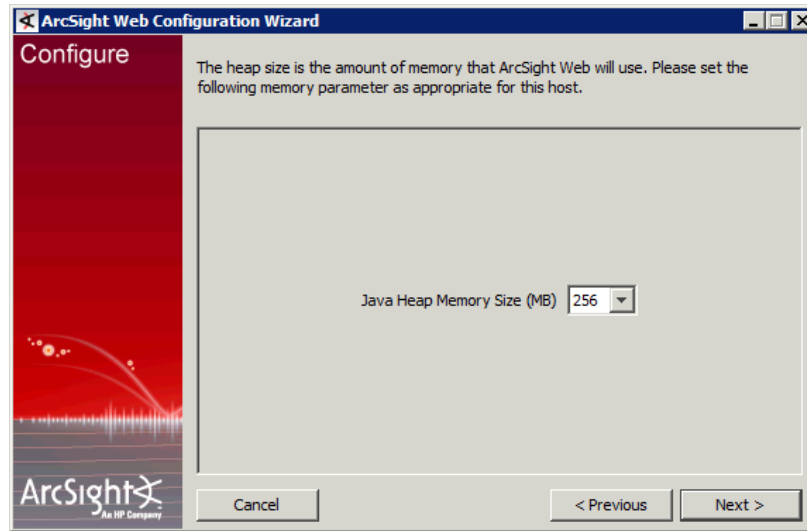
## Web Server Host Name and Port

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.



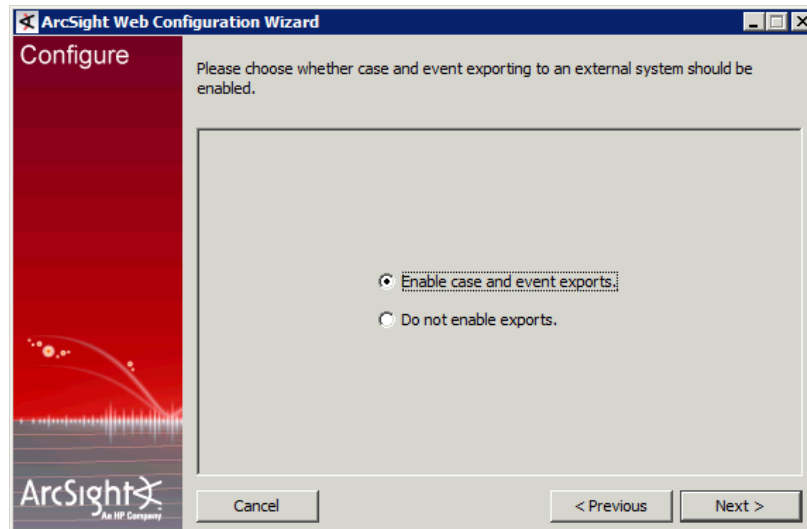
## Java Heap Memory Size

Select the heap memory size and click **Next**.



## Enable Case and Events Exports

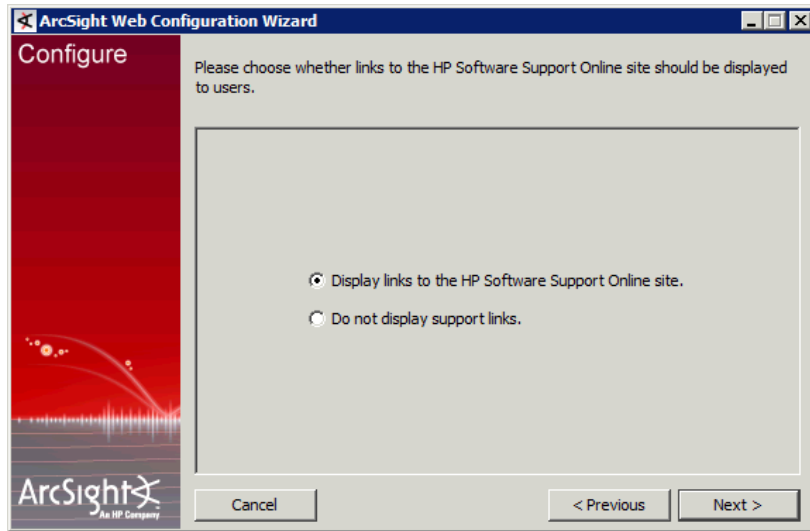
If you want to export cases and events, select **Enable case and event exports**.



Click **Next**.

## Display Links to Support Web site

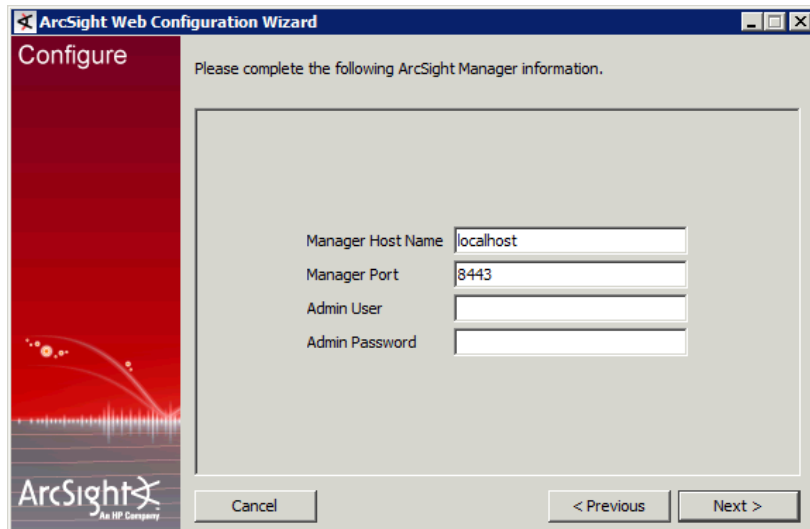
Choose whether to display a link to Customer Support on the home page. and click **Next**.



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 and the text 'An HP Company'. The main content area has a light gray background. At the top, it says 'Please choose whether links to the HP Software Support Online site should be displayed to users.' Below this, there are two radio button options: 'Display links to the HP Software Support Online site.' (which is selected) and 'Do not display support links.' At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

## ArcSight Manager Host Name and Port

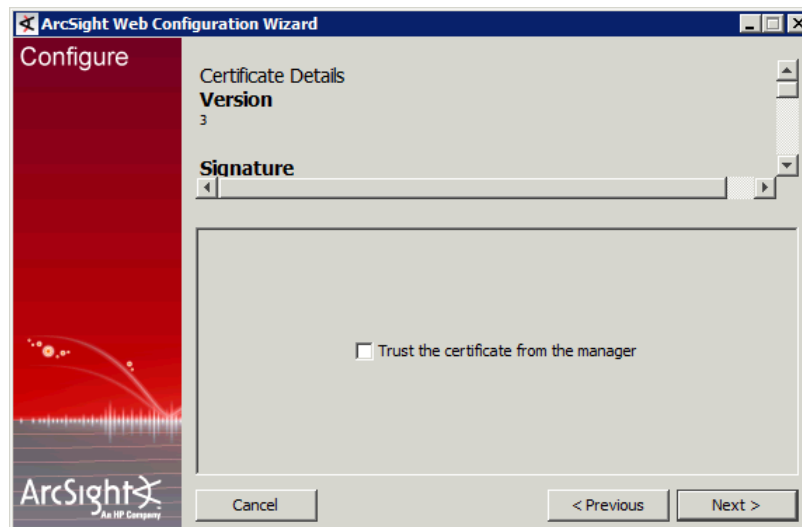
Make sure that the Manager is up and running. Then, enter the ArcSight Manager's host name, port, admin user and admin password and click **Next**.



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 and the text 'An HP Company'. The main content area has a light gray background. At the top, it says 'Please complete the following ArcSight Manager information.' Below this, there are four input fields: 'Manager Host Name' (with 'localhost' entered), 'Manager Port' (with '8443' entered), 'Admin User' (empty), and 'Admin Password' (empty). At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

## 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**

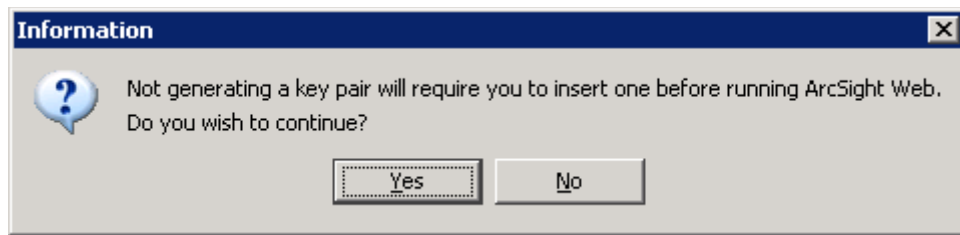


## Select Type of Key Pair

You will be prompted to select the type of key pair you want to use. Make your selection and click **Next**:



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:

A screenshot of the "ArcSight Web Configuration Wizard" window, titled "Configure". The left sidebar is red with the ArcSight logo and the text "An HP Company". 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 are several input fields: "Validity (days)" with the value "365", "Country", "State", "Locality", "Organization", and "Organizational Unit". At the bottom are three buttons: "Cancel", "< Previous", and "Next >".

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

A screenshot of the "ArcSight Web Configuration Wizard" window, titled "Configure". The left sidebar is red with the ArcSight logo and the text "An HP Company". 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 Web." Below this text are two input fields: "SSL key store password" and "Password Confirmation". At the bottom are three buttons: "Cancel", "< Previous", and "Next >".

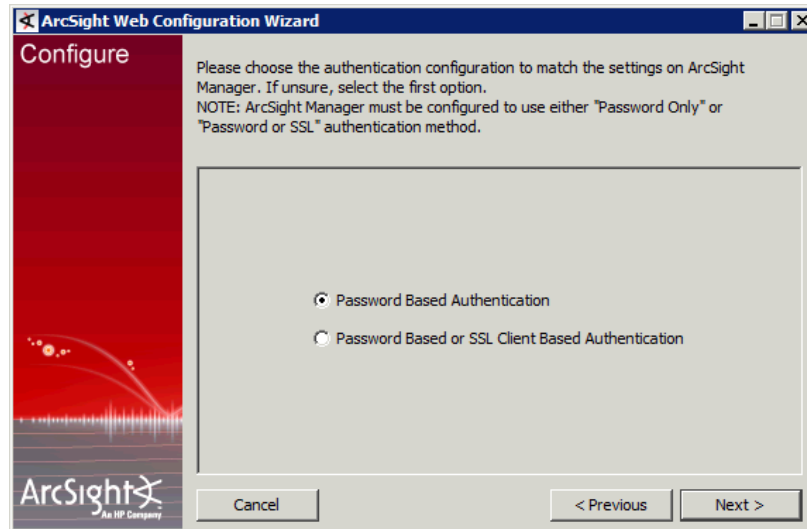
If you selected the **Demo key pair** option, you will also see the screen above that prompts you for a password for the SSL Key store used by ArcSight Web.

## Authentication

Choose the type of client authentication you want to use and click **Next**.



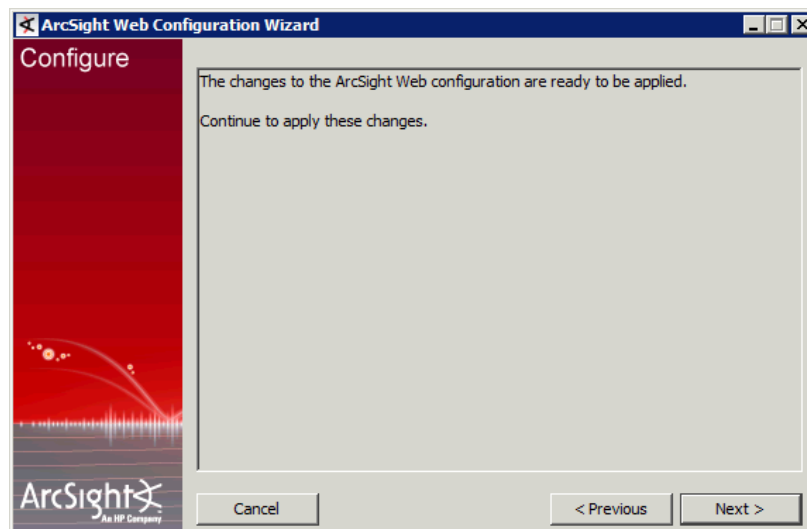
If you plan to use a PKCS #11 token with ArcSight Web, be sure to select **Password Based or SSL Client Based Authentication** and make sure that your Manager is configured to use this authentication method too.



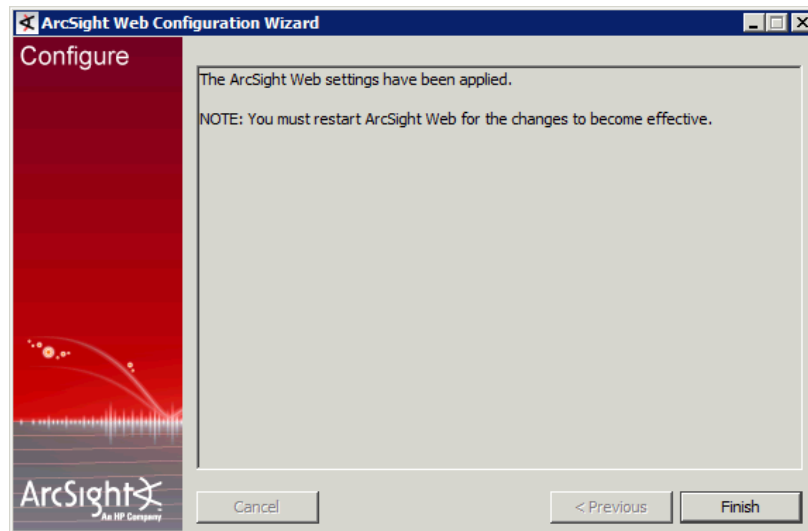
## Setting ArcSight Web as a Service or Daemon

Choose whether ArcSight Web should be installed as service or not and click **Next**.

You will see the following screen:



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



Click **Finish** to save changes.

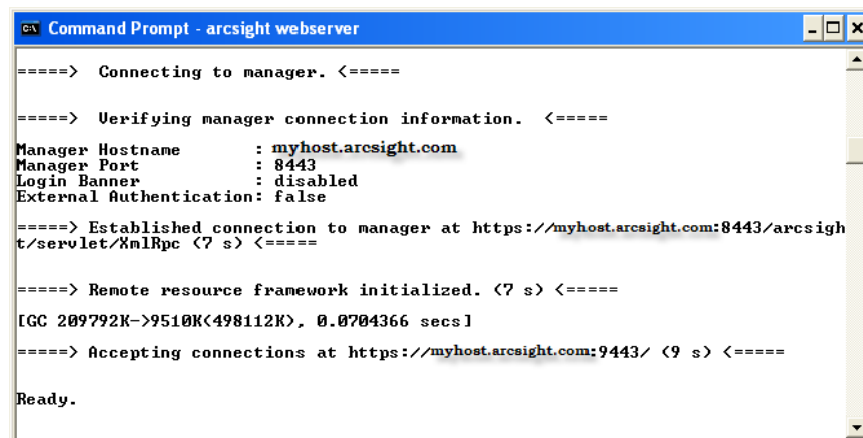
The next screen gives you the location where ArcSight Web has been installed. Click **Done**.

## Starting ArcSight Web Manually

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

```
arcsight webserver
```

When you start up, the web 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 webserver has started successfully.



## Connecting to ArcSight Web

Go to this web site (fill in the appropriate host name):

<https://<hostname>:9443/arcsight/app>, 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, run the **Start->All Programs->ArcSight Web ->Uninstall ArcSight Web 5.6** program. 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 Linux 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 141](#)

[“Installing SmartConnectors” on page 141](#)

After you have installed the ArcSight Manager, you should install SmartConnectors for all of the devices that you want ESM 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 SmartConnectors require you to configure the device before you can receive events.

For more information on how to install a particular SmartConnector and configure the device, refer to the SmartConnector User's Guide for basic SmartConnector installer instructions and also refer to the vendor-specific 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 SmartConnectors.

HP 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 HP, the 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 SmartConnectors

Before installing SmartConnectors, confirm that the ArcSight Manager and Database components are up and running. Log in as user *arcsight*, or an existing user with sufficient admin privileges. Install 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 v5.6 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.

When the ESM Manager is installed in FIPS with Suite B compliant mode, the SmartConnectors must also be installed in FIPS with Suite B compliant mode.

# Establishing Initial ArcSight Resources

---

This chapter describes the initialization of resources in a new ESM 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 143](#)

[“Defining Asset Categories” on page 146](#)

[“Creating Customers and Users” on page 147](#)

[“Tuning Data Monitors and Rules” on page 147](#)

To complete your ESM 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 ESM 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 prompt '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"/>

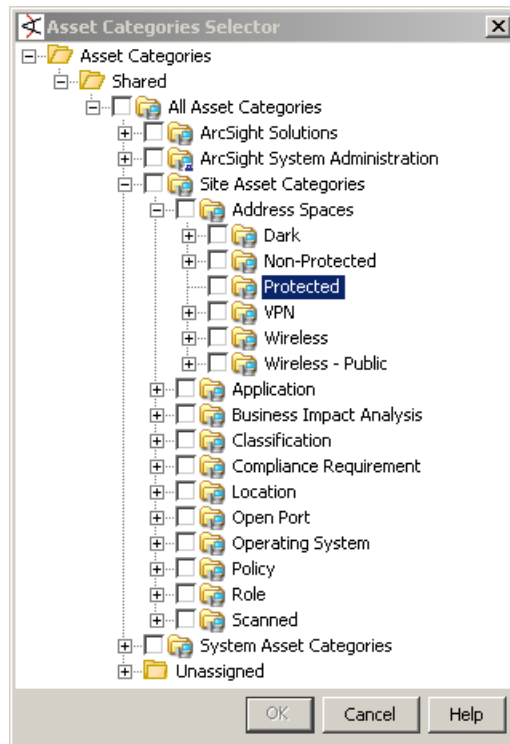
Assign	
Owner	
Notification Groups	

(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.

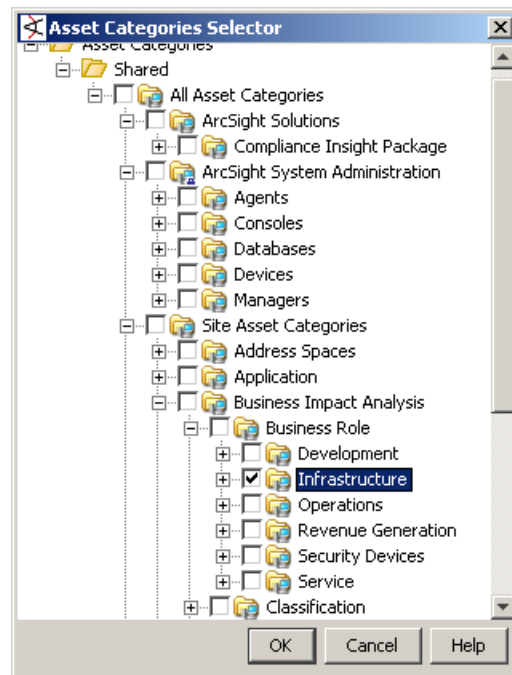


- 8 Update your SmartConnectors to use the Zones you have defined. Examine each SmartConnector in the Navigator pane and select **Configure** from the context menu. On the Networks tab, make sure that the SmartConnector is associated with the appropriate Network resources.

## 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 ESM 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 ESM 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.

# 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 20130101 thru 20130105 in that order and you want to reactivate partitions 20130101 thru 20130103, you must start by reactivating 20130101 first, then 20130102 and lastly 20130103.

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, 2013, a subdirectory named `arc_event_20130401` 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.

We recommend 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, 2013 is `20130401`.  
  
`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 20130401. The Archive Directory is E:\archive.

- 1 List the data files in the subdirectory for the partition 20130401:

```
E:\archive>dir arc_event_20130401

Directory of E:\archive\arc_event_20130401

05/09/2013  1,728                arc_event_data_20130401.dmp
05/09/2013   560                arc_event_data_20130401.exp.log
05/09/2013 3,823,657,634        arc_event_data_20130401_01.dbf
05/09/2013 3,657,584,358        arc_event_data_20130401_02.dbf
05/09/2013 3,657,584,287        arc_event_data_20130401_03.dbf
```

- 2 Archive the subdirectory for the partition (arc\_event\_20130401) with the command-line version of WinZip with AES256 encryption:

```
E:\archive>"C:\Program Files\WinZip\WZZIP.EXE" -P -s -ycAES256
arc_event_20130401.zip arc_event_20130401

Adding arc_event_20130401\arc_event_data_20130401.dmp
Adding arc_event_20130401\arc_event_data_20130401.exp.log
Adding arc_event_20130401\arc_event_data_20130401_01.dbf
Adding arc_event_20130401\arc_event_data_20130401_02.dbf
Adding arc_event_20130401\arc_event_data_20130401_03.dbf
creating Zip file arc_event_20130401.zip
```

- 3 Generate the SHA1 signature for the archive file arc\_event\_20130401.zip with cygwin's sha1sum command:

```
E:\archive>sha1sum arc_event_20130401.zip >
arc_event_20130401.SHA1
```

**Example 2:** In this example the partition (20130401) archived in the previous example is reactivated. The Archive Directory is E:\archive.

- 1 Unzip the archive file arc\_event\_20130401.zip with WinZip command line version to restore the files:

```
E:\archive>"C:\Program Files\WinZip\WZUNZIP.EXE" -d -s
arc_event_20130401.zip
```

Zip file: arc\_event\_20130401.zip

unzipping arc\_event\_20130401\arc\_event\_data\_20130401.dmp

unzipping arc\_event\_20130401\arc\_event\_data\_20130401.exp.log

unzipping arc\_event\_20130401\arc\_event\_data\_20130401\_01.dbf

unzipping arc\_event\_20130401\arc\_event\_data\_20130401\_02.dbf

unzipping arc\_event\_20130401\arc\_event\_data\_20130401\_03.dbf

- 2 List the contents of the arc\_event\_20130401 subdirectory to make sure data files have been extracted:

E:\archive>dir arc\_event\_20130401

Directory of E:\archive\arc\_event\_20130401

05/09/2013 1,728 arc\_event\_data\_20130401.dmp

05/09/2013 560 arc\_event\_data\_20130401.exp.log

05/09/2013 3,823,657,634 arc\_event\_data\_20130401\_01.dbf

05/09/2013 3,657,584,358 arc\_event\_data\_20130401\_02.dbf

05/09/2013 3,657,584,287 arc\_event\_data\_20130401\_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 ESM authentication mechanism that stores password information in the ArcSight Database. This appendix covers the following topics:

[“Passcodes” on page 153](#)

[“Defining Shorter ESM Internal Login User Names” on page 153](#)

[“Two-Factor Challenge Responses” on page 154](#)

[“Steps for Setting Up ACE/Server RADIUS Authentication” on page 155](#)

[“Installing the ACE/Server and ACE/Server RADIUS Service” on page 155](#)

[“Configuring the ACE/Server to allow RADIUS Requests” on page 155](#)

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 ESM 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 ESM in some cases. Challenges are requests for additional user input that the Two-Factor Authentication server will send to HP during the authentication process.

This challenge mechanism works in the following components of the ESM 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 81](#) 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.



Note

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, see ["Guidelines for setting up external authentication" on page 92](#).

## 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
```

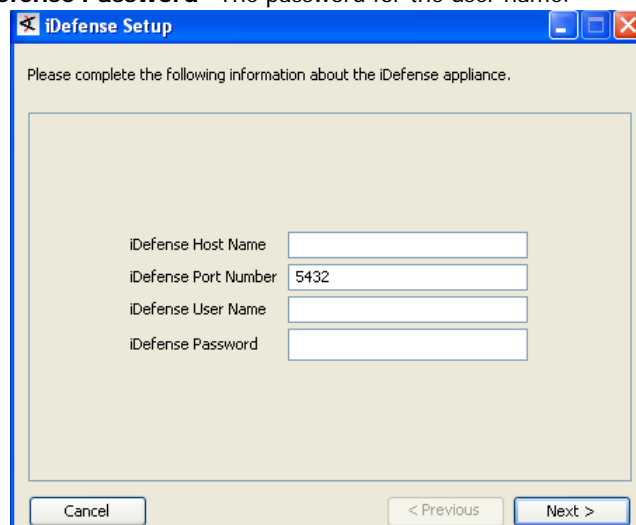
- 2 Enter this information in the wizard that launches:

**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 is a large rectangular frame containing four input fields: 'iDefense Host Name' (empty), 'iDefense Port Number' (containing '5432'), 'iDefense User Name' (empty), and 'iDefense Password' (empty). At the bottom of the dialog are three buttons: 'Cancel' on the left, '< Previous' in the center, and 'Next >' on the right.

- 3 Click **Next**.



## Appendix D

# 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 161](#)

[“Starting Processes” on page 164](#)

[“Monitoring Processes” on page 164](#)

[“Next Steps” on page 165](#)

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 Protect 724 site.

Note

---

## 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.

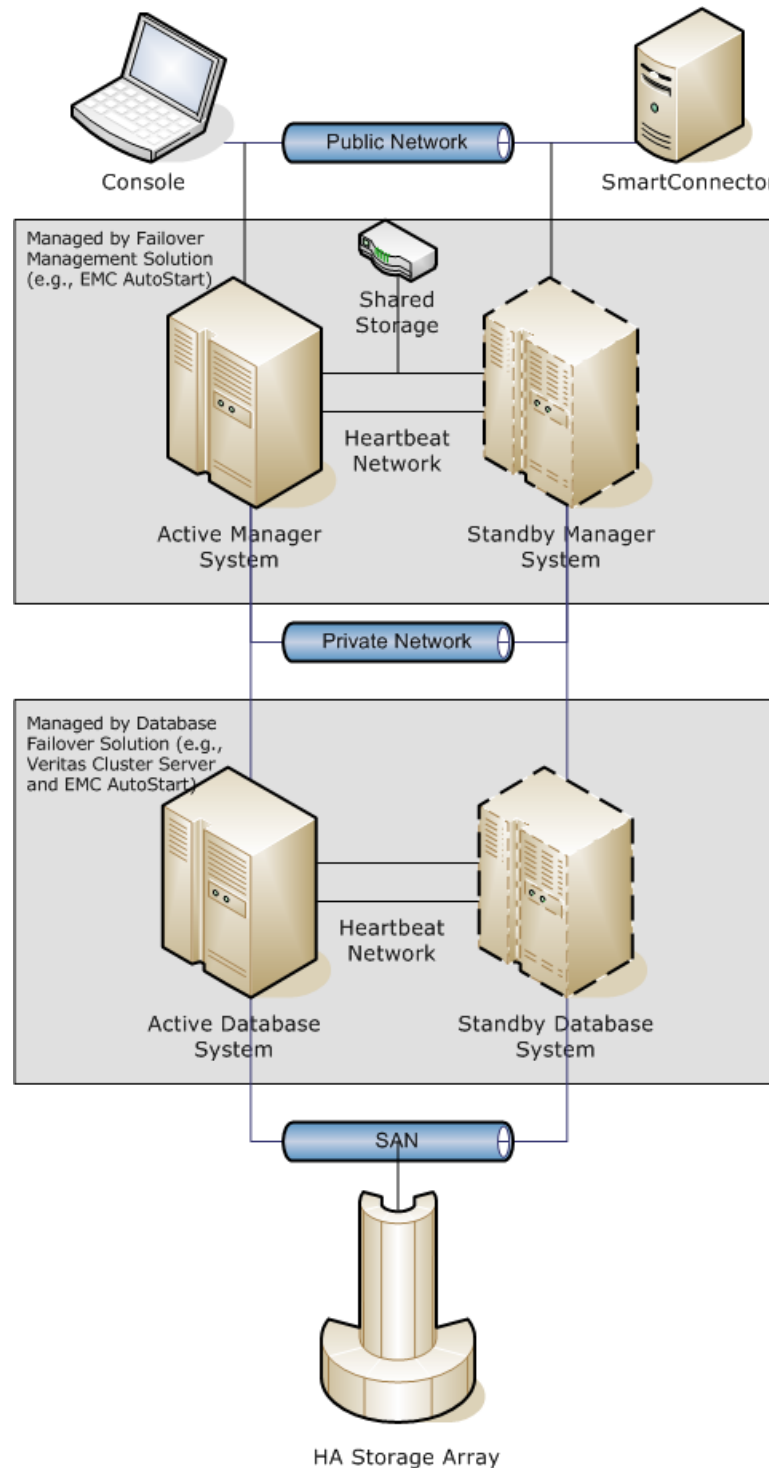
ArcSight Managers don't use write caches--this means that all writes always immediately go through to the database. They do, however, use read caches. They do not poll the database for changes of the data as it would be too expensive. For this reason, you must not connect two ArcSight Manager instances 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 D-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. (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. We provide 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.



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 E

# FIPS Compliant State Auditing

---

This appendix covers the following topics:

[“Compliance State Auditing with Active Channels” on page 167](#)

[“Compliance State Auditing with Dashboards” on page 168](#)

[“Compliance State Auditing with Reports” on page 168](#)

[“Compliance State Auditing with Rules” on page 169](#)

Because ESM 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 ArcSight 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 167](#)
- [“Compliance State Auditing with Dashboards” on page 168](#)
- [“Compliance State Auditing with Reports” on page 168](#)
- [“Compliance State Auditing with Rules” on page 169](#)

## 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 Of 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 Of 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 168](#).
  - 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 ArcSight 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 167](#).
  - 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 168](#) and click **Apply**.
- 2 In the Reports tab, create a new report and add the query you created in [Step 1 on page 169](#).

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 168](#) 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 ESM in FIPS Mode

---

This section covers the following topics:

- [“What is FIPS?” on page 172](#)
- [“Network Security Services Database \(NSS DB\)” on page 172](#)
- [“What is Suite B?” on page 173](#)
- [“NSS Tools Used to Configure Components in FIPS Mode” on page 173](#)
- [“TLS Configuration in a Nutshell” on page 174](#)
- [“Using PKCS #11 Token With a FIPS Mode Setup” on page 176](#)
- [“Installing ArcSight Database” on page 177](#)
- [“Installing the ArcSight Manager in FIPS mode” on page 177](#)
- [“Setting up Partition Archiver in FIPS Mode” on page 183](#)
- [“Installing ArcSight Console in FIPS Mode” on page 184](#)
- [“Configure Your Browser for FIPS” on page 197](#)
- [“Installing ArcSight Web in FIPS Mode” on page 190](#)
- [“Installing SmartConnectors in FIPS mode” on page 197](#)
- [“How do I Know if My Installation is FIPS Enabled?” on page 198](#)

ESM supports the Federal Information Processing Standard 140-2 (FIPS 140-2) and Suite B. You can choose to install the product components in FIPS mode if you have the requirement to do so.



Before installing ESM in FIPS mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled ArcSight Manager.

This section provides you instructions for installing ESM in FIPS mode.

To install ESM in default mode, follow the instructions in the respective chapters for installing the components.

To install ESM in FIPS with Suite B mode, follow the instructions in [Appendix G, Installing ESM in FIPS with Suite B Mode, on page 201](#).

Section [“Differences Between Default and FIPS Modes” on page 21](#) lists the basic differences between the three modes.



**Note**

When the ArcSight Manager is installed in FIPS mode, all other components must also be installed in FIPS mode.

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

---

## What is FIPS?

FIPS 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 components configured in the FIPS 140-2 mode. Even though an ArcSight 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. We recommend that you run all components in FIPS mode in order to be fully FIPS 140-2 compliant.

---

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 you use 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 ArcSight Manager
- <ARCSIGHT\_HOME>\current\config\nssdb.client on the ArcSight Console
- <ARCSIGHT\_HOME>\config\jetty\webnssdb on ArcSight Web
- <ARCSIGHT\_HOME>\user\agent\nssdb.client on ArcSight Database



The default password for the NSS DB on every component is *changeit*. However, we recommend that you change this password by following the procedure in section “Changing the Password for NSS DB” in the Administrator’s Guide.

## What is Suite B?

Suite B is a set of cryptographic algorithms put forth by the National Security Agency (NSA) as part of the national cryptographic technology. While FIPS 140-2 supports sensitive but unclassified information, FIPS with Suite B supports both unclassified information and most classified up to top secret information. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.



- Not all ESM versions support the FIPS with Suite B mode. Refer to the ESM Product Lifecycle Document available on the Protect 724 website for supported platforms for FIPS with Suite B mode.
- When the Manager is installed in FIPS with Suite B compliant mode, all components (ArcSight Web, ArcSight Console, SmartConnectors, and Logger, if applicable) must be installed in FIPS with Suite B compliant mode, and browser used to access ESM must be FIPS enabled.
- ArcSight Web that will be connecting to a ArcSight Manager installed in FIPS with Suite B mode must also be installed in FIPS with Suite B mode.
- Before installing ESM in FIPS with Suite B mode, keep in mind that pre-v4.0 Loggers will not be able to communicate with a FIPS-enabled ArcSight Manager.

When configured to use Suite B mode, ESM supports Suite B Transitional profile. There are 2 level of security defined in Suite B mode:

- **TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA**  
Suite B 128-bit security level, providing protection from unclassified up to secret information
- **TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA**  
Suite B 192-bit security level, providing protection from unclassified up to top secret information.

## NSS Tools Used to Configure Components in FIPS Mode

NSS is a cross-platform cryptographic C library and a collection of security tools. 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.
- **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).

See “Appendix A, Administrative Commands” in the 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:

On Windows:

```
arcsight.bat <command_name> -H
```

On Linux:

```
./arcsight <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 ArcSight Manager, Partition Archiver, ArcSight Console, and ArcSight 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 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 the ArcSight Manager in FIPS mode” on page 177](#)
- [“Setting up Partition Archiver in FIPS Mode” on page 183](#)
- [“Installing ArcSight Console in FIPS Mode” on page 184](#)
- [“Installing ArcSight Web in FIPS Mode” on page 190](#)

Refer to the Administrator’s Guide for information on upgrading an existing default mode installation into FIPS mode.

## Understanding Server Side Authentication

The first step in an SSL handshake is when the server (ArcSight Manager) authenticates itself to the client (ArcSight Console, ArcSight Web). This is called server side authentication. To set up TLS configuration on your ArcSight Manager for server side authentication, you need:

- A key pair in your ArcSight Manager's NSS DB. You can generate a new key pair or use an existing key pair.
- The ArcSight Manager's certificate, which incorporates the public key from the key pair located in the ArcSight Manager's NSS DB. You can use one of the following:
  - ◆ A self-signed certificate which you generate in the ArcSight Manager's NSS DB and sign yourself
  - ◆ A CA-signed certificate which should be imported into the ArcSight Manager's NSS DB
  - ◆ An existing self-signed or CA-signed certificate which should be imported into the ArcSight Manager's NSS DB

Next, you should export the ArcSight 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 ArcSight Manager. If the ArcSight Manager has a CA-signed certificate, you have to import the CA's certificate instead of the ArcSight 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 (ArcSight Manager) has authenticated itself to the client (ArcSight Console or ArcSight Web). At this point, the server requests the client to authenticate itself.

For the ArcSight Console to authenticate itself to the ArcSight Manager, you should have the following in the ArcSight Console's NSS DB:

- A key pair. You can either:
  - ◆ Generate a new key pair in the ArcSight Console's NSS DB, or
  - ◆ Use an existing key pair which should be imported into the ArcSight Console's NSS DB
- The ArcSight Console's certificate, which incorporates the ArcSight Console's public key. You can use one of the following:
  - ◆ a new CA-signed certificate which should be imported into the ArcSight Console's NSS DB
  - ◆ an existing certificate which should be imported into the ArcSight Console's NSS DB

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 ArcSight Manager's NSS DB as the token is a client to the ArcSight Manager.

For detailed procedures on each of the steps mentioned above, refer to the section, "Setting up Client-Side Authentication" in the 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 ArcSight Manager to which it connects. On the other, it acts as a server to web browsers that connect to it. Therefore, ArcSight Web authenticates the ArcSight Manager but has to authenticate itself to web browsers.

To authenticate the ArcSight Manager, ArcSight Web should have either the ArcSight Manager's certificate (if the ArcSight Manager is using a self-signed certificate) or the certificate of the CA that signed the ArcSight Manager's certificate (if the ArcSight 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.

The web browsers that try to connect to ArcSight Web import ArcSight Web's certificate into their truststore and use it to trust the webserver.

This topic does not apply to ArcSight Console, which automatically imports the certificate. In a nutshell, you have to:

- Import the ArcSight Manager's certificate (in the case of self-signed certificate on the ArcSight Manager) or the certificate of the CA that signed the ArcSight Manager's certificate (in the case where ArcSight Manager is using a CA-signed certificate) into the Web's NSS DB.
- Have a key pair in ArcSight 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 ArcSight Web's NSS DB. You can use one of the following:
  - ◆ A new self-signed certificate which you generate in the ArcSight Web's NSS DB and sign yourself
  - ◆ A new CA-signed certificate which needs to be imported into the ArcSight Web's NSS DB
  - ◆ An existing self-signed or CA-signed certificate which needs to be imported into the ArcSight Web's NSS DB

## Using PKCS #11 Token With a FIPS Mode Setup

To use a PKCS #11 Token, such as the ActivClient's Common Access Card (CAC), follow the steps below.

For details on any of these steps, see [Appendix H, Using the PKCS#11 Token, on page 215](#).

- 1 Install the CAC provider's software on each client machine. That includes the ArcSight Console and every machine using a browser to access ArcSight Web or the Management Console. See ["Install the CAC Provider's Software" on page 216](#).
- 2 Export the CAC card's certificate from the card.
- 3 Extract the root CA's certificate from the CAC card's certificate.
- 4 Import the CAC card's certificate and root CA's certificate into the ArcSight Manager's nssdb and web server webnssdb.

## Installing ArcSight Database

The steps to install ArcSight Database are the same regardless of the mode in which you want to install ESM. So, follow the instructions in the chapter, [“Installing ArcSight Database” on page 33](#) to install the Database.

## Installing the ArcSight Manager in FIPS mode

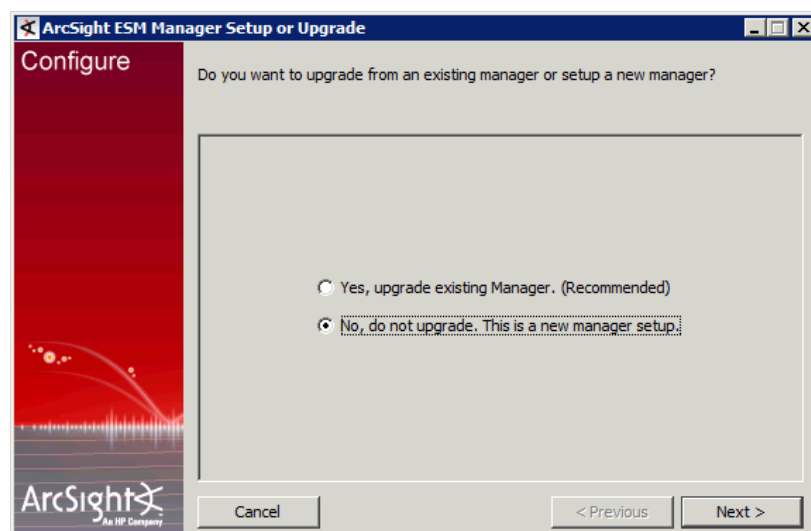
The ArcSight Manager requires that the ArcSight Database be installed prior to installing the ArcSight Manager.

This section instructs you on installing the ArcSight Manager in FIPS mode only. For steps to install the ArcSight Manager in default mode, refer to the chapter, [“Installing ArcSight Manager” on page 81](#). The [Installing ArcSight Manager](#) chapter also lists the supported platforms for the ArcSight Manager and contains information that is common to both FIPS mode and default mode. You can also refer to the ESM Product Lifecycle document available on the Protect 724 website for supported platforms.

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 Administrator’s Guide for details on obtaining and using a CA-signed certificate.

To install the ArcSight Manager:

- 1 Create a user called *arcsight* to own the installation. (See [“About the ArcSight User” on page 83](#).)
- 2 Log in as user *arcsight* before running the ArcSight 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 window.
- 7 Generate a key pair on the ArcSight 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 ArcSight Manager's key pair and certificate get generated and stored in its `nssdb`. The ArcSight Manager's public key is embedded in its certificate, thereby linking the ArcSight 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 ArcSight Manager's `<ARCSIGHT_HOME>/config/jetty/nssdb`.

This key pair should be exported in `.pfx` format and then imported into the ArcSight Manager's NSS DB. Refer to the section, "Using Keytoolgui to Export a Key pair," in the Administrator's Guide for details on exporting a key pair.

Refer to the section, "Importing an Existing Key pair into the ArcSight Manager's NSS DB" in the Administrator's Guide for detailed steps on doing this.

- When you import or generate a key pair into `nssdb`, if there is an 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 ArcSight Manager's `<ARCSIGHT_HOME>/bin` directory to generate a key pair. This will automatically generate the ArcSight 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` to set the validity period of your certificate is optional. If you do not use this option, the certificate will be valid for 3 months by default. If you choose to use it, see ["Setting the Expiration Date of a Certificate" on page 213](#) section in the Administrator's Guide for additional information.
- For the `-t` option, be sure to use C,C,C protocols only as shown in the command.
- The hostname is the short name or fully qualified domain name depending upon how your ArcSight Manager name was set up when you installed the ArcSight Manager.

```
./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
```

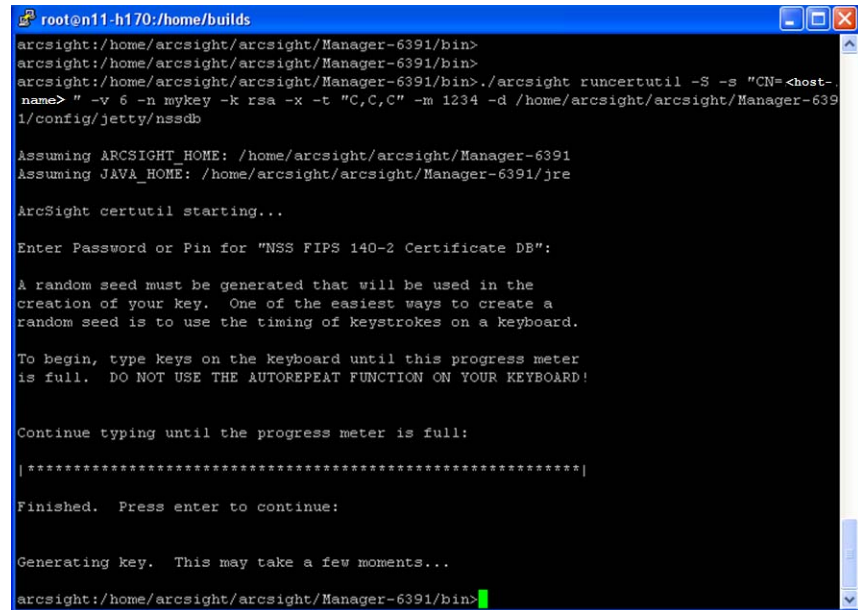
For example, if your hostname is `host.arcsight.com`, you would run:

```
./arcsight runcertutil -S -s "CN=host.arcsight.com" -v 6 -n
mykey -k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/nssdb
```

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.

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 ArcSight Manager's nssdb.



```
root@n11-h170:/home/builds
arcsight:/home/arcsight/arcsight/Manager-6391/bin>
arcsight:/home/arcsight/arcsight/Manager-6391/bin>
arcsight:/home/arcsight/arcsight/Manager-6391/bin> ./arcsight runcertutil -S -s "CN=host-
name" -v 6 -n mykey -k rsa -x -t "C,C,C" -m 1234 -d /home/arcsight/arcsight/Manager-639
1/config/jetty/nssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Manager-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Manager-6391/jre

ArcSight 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:

| *****|

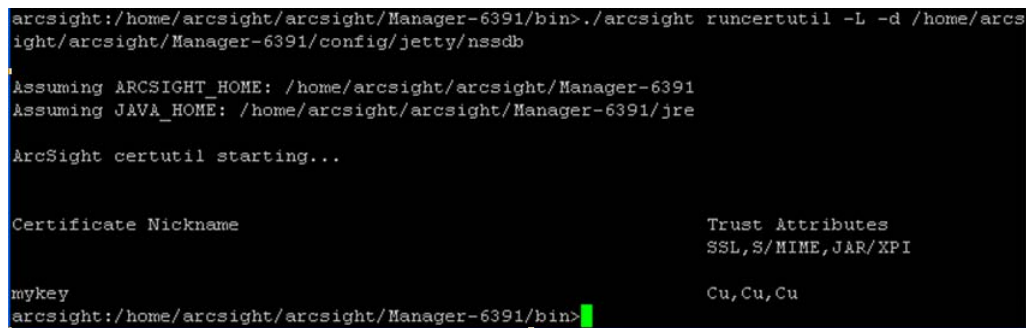
Finished. Press enter to continue:

Generating key. This may take a few moments...

arcsight:/home/arcsight/arcsight/Manager-6391/bin>
```

- b** To check whether the key pair has been successfully created in the nssdb, run the following from the ArcSight Manager's <ARCSIGHT\_HOME>/bin directory:

```
./arcsight runcertutil -L -d
<ARCSIGHT_HOME>/config/jetty/nssdb
```



```
arcsight:/home/arcsight/arcsight/Manager-6391/bin> ./arcsight runcertutil -L -d /home/arcs
ight/arcsight/Manager-6391/config/jetty/nssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Manager-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Manager-6391/jre

ArcSight certutil starting...

Certificate Nickname                                Trust Attributes
SSL,S/MIME,JAR/XPI

mykey                                                Cu,Cu,Cu
arcsight:/home/arcsight/arcsight/Manager-6391/bin>
```

- 8** Export the ArcSight Manager's certificate.

You are required to have this exported certificate handy when installing the clients (ArcSight Console and/or ArcSight Web) that will be connecting to this ArcSight Manager. You have to import this certificate into the clients' NSS DB (<ARCSIGHT\_HOME>/current/config/nssdb.client in case of the ArcSight Console and <ARCSIGHT\_HOME>/config/jetty/webnssdb in case of ArcSight Web) when installing them. Importing the ArcSight Manager's certificate allows the clients to trust the ArcSight Manager.

To export the ArcSight Manager's certificate, run the following command from the ArcSight Manager's <ARCSIGHT\_HOME>/bin directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o <absolute_path_to
_Manager's_certificate>
```



The -o specifies the absolute path to the location where you want the exported ArcSight Manager's certificate to be placed. If you do not specify the absolute path the file will be exported to your <ARCSIGHT\_HOME> directory by default.

For example, to export the ArcSight Manager's certificate as a file named ManagerCert.cer to /home/arcsight/arcsight/Manager directory, run:

```
./arcsight runcertutil -L -n mykey -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o
/home/arcsight/arcsight/Manager/ManagerCert.cer
```

This exports the ManagerCert.cer file, the ArcSight Manager's certificate, in /home/arcsight/arcsight/Manager directory.

```
arcsight:/home/arcsight/arcsight/Manager-6391/bin>./arcsight runcertutil -L -n mykey -r -d
/home/arcsight/arcsight/Manager-6391/config/jetty/nssdb -o /home/arcsight/arcsight/Manager-6391/ManagerCert.cer

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Manager-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Manager-6391/jre

ArcSight certutil starting...

arcsight:/home/arcsight/arcsight/Manager-6391/bin>
```

## 9 (Only if you plan to use CAC with this ESM setup)

If you plan to use CAC with the ArcSight Console or ArcSight Web, you need to import the CAC card's CA's root certificate into the ArcSight Manager's nssdb. See the sections ["Obtain the CAC's Issuers' Certificate" on page 218](#) and ["Extract the Root CA Certificate From the CAC Certificate" on page 220](#) for details on how to obtain the CAC card's CA's root certificate.

To import the CAC card's CA's root certificate into the ArcSight Manager: run

```
./arcsight runcertutil -A -n CACcert -t "CT,C,C" -d
<ARCSIGHT_HOME>/config/jetty/nssdb -i
<absolute_path_to_the_root_certificate>
```

```
arcsight:/home/arcsight/arcsight/Manager-6391/bin>./arcsight runcertutil -A -n CACcert -t
"CT,C,C" -d /home/arcsight/arcsight/Manager-6391/config/jetty/nssdb -i /home/arcsight/arcsight/Manager-6391/cac-root-cert.cer

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Manager-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Manager-6391/jre

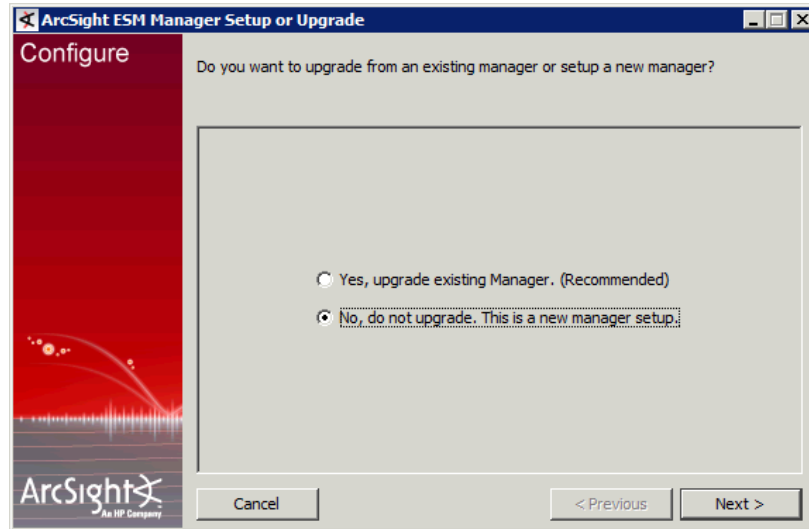
ArcSight certutil starting...

arcsight:/home/arcsight/arcsight/Manager-6391/bin>
```

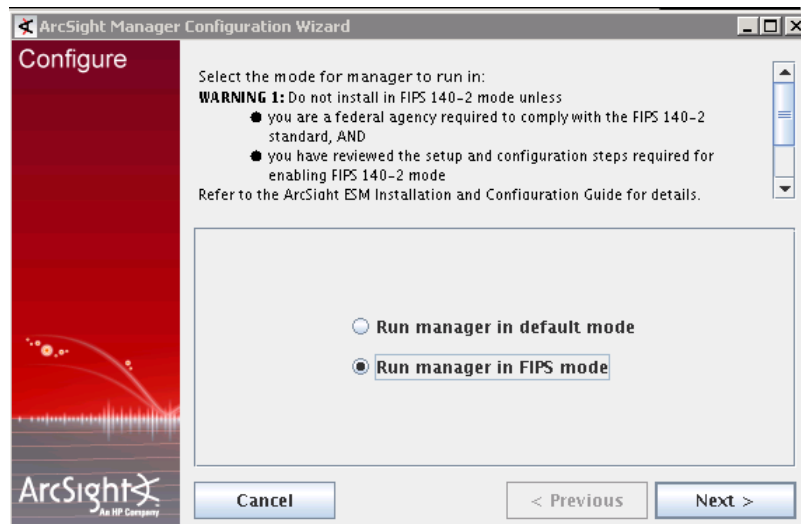


For the -t option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 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**.

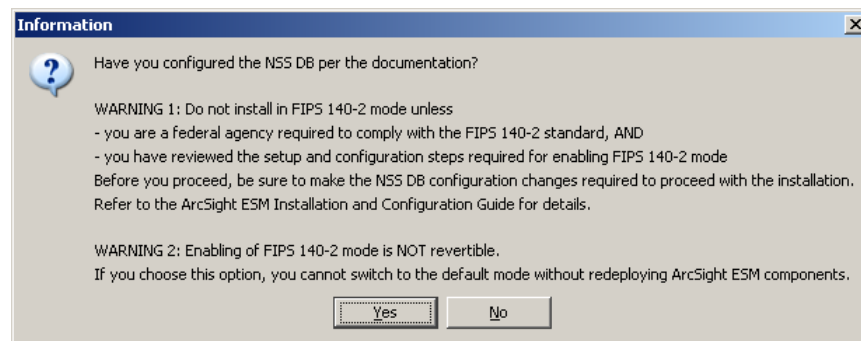


- 11 Next, you will see the following screen:

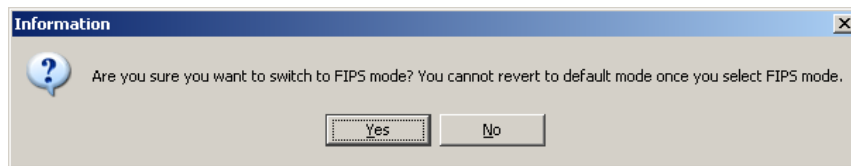


Select the **Run manager in FIPS mode** radio button and click **Next**.

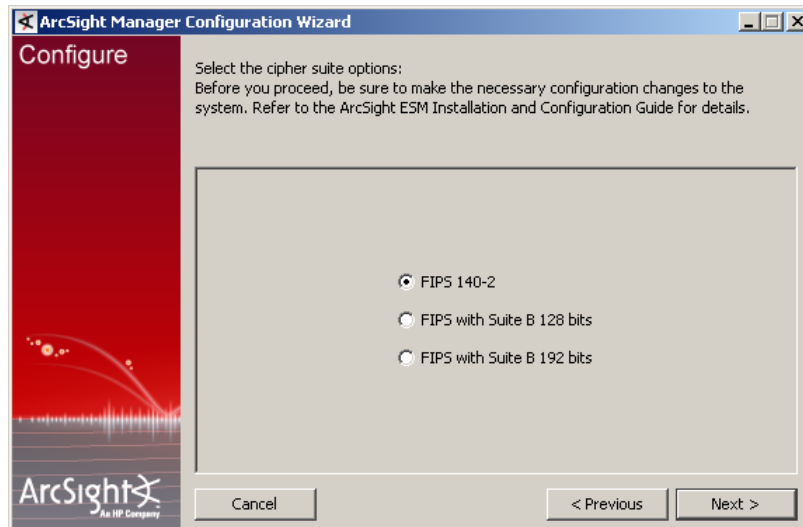
- 12 The configuration wizard will ask you to confirm that you have set up the NSS DB. Click **Yes** since you have already generated a keypair in the ArcSight Manager's NSS DB.



- 13 You will be reminded that once you select the FIPS mode, you will not be able to revert to the default mode. Click **Yes**.



- 14 Starting in ESM v5.0, you can opt to install the ArcSight Manager in FIPS with Suite B mode. The next screen asks you to select the cipher suite of your choice. Select **FIPS 140-2** and click **Next**.



- 15 Follow the prompts in the next few screens until you get to the screen that prompts you to select an authentication setup. Refer to the chapter, "[Installing ArcSight Manager](#)" on page 81 for details on any screen.



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 ArcSight Console only:

You can set the authentication option on the ArcSight Manager to **Password Based or SSL Client Based Authentication** or **SSL Client Only Authentication**.

- ◆ If you plan to use CAC with ArcSight Web only or ArcSight Web and ArcSight Console:

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

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

- 16 Follow the prompts in the next few wizard screens to complete the ArcSight Manager installation. Refer to [Installing ArcSight Manager](#) chapter for details on any screen.
- 17 Start the ArcSight Manager by entering the following from the ArcSight Manager's /bin directory:

```
./arcsight manager
```

When the ArcSight Manager starts up, it will display a stream of messages in the terminal window to reflect its status.

## 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 33](#) 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 Linux 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 ArcSight Manager, so it must be configured to trust the ArcSight Manager that it will be connecting to. To configure Partition Archiver, you have to import the ArcSight Manager's certificate into the ArcSight Database's `nssdb.client`. To import the ArcSight Manager's certificate:

- 1 Make sure you are logged in as the Oracle software owner.
- 2 Open a shell/command prompt window.
- 3 Execute the following command to import the ArcSight 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>
```

```
root:/usr/local/arcsight/db-6391/bin>./arcsight runcertutil -A -n ManagerCert -t "C
T,C,C" -d /usr/local/arcsight/db-6391/user/agent/nssdb.client -i /home/arcsight/Man
agerCert.cer

Assuming ARCSIGHT_HOME: /usr/local/arcsight/db-6391
Assuming JAVA_HOME: /usr/local/arcsight/db-6391/jre

ArcSight certutil starting...

root:/usr/local/arcsight/db-6391/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 ArcSight 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.client
```
- 5 From the ArcSight Database's <ARCSIGHT\_HOME>/bin, run the setup program:
 

```
./arcsight agentsetup -w
```
- 6 Select **Run Connector in FIPS 140-2 mode** when prompted.
- 7 Since you have already imported the ArcSight Manager's certificate into the database's nssdb.client, 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, run them from the ArcSight Manager's <ARCSIGHT\_HOME>\bin directory instead of from the ArcSight Database's /bin directory.

- 8 Follow the prompts in the next few wizard screens to complete the Partition Archiver set up. Refer to ["Setting Up Partition Archiver" on page 77](#) for details on any screen.

## Installing ArcSight Console in FIPS Mode



If you would like to set up client-side authentication on the ArcSight Console, refer to the Administrator's Guide for detailed steps to do so.

Install and test the ArcSight Database and ArcSight 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 ESM Product Lifecycle document available on the Protect 724 website (<https://protect724.arcsight.com>) for details on supported platforms for the ArcSight Console.

This section tells you how to install the ArcSight Console in FIPS mode only. For details on installing the ArcSight Console in default mode, refer to the “Installing ArcSight Console” chapter, earlier in this guide.

In order for an ArcSight Console to communicate with a FIPS enabled ArcSight Manager, the ArcSight Console must trust the ArcSight Manager. This trust is established by importing the ArcSight Manager's certificate into the ArcSight Console's NSS DB (<ARCSIGHT\_HOME>\current\config\nssdb.client). After you configure the ArcSight Console for FIPS, it will automatically import the ArcSight Manager's certificate the first time you start it.

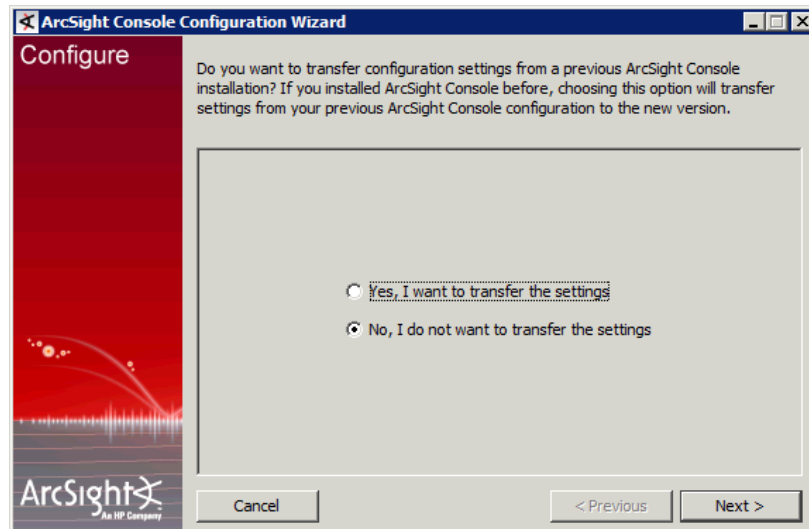


Note

If your ArcSight Manager is installed on a different machine than the machine on which you will be installing the ArcSight Console, make sure to copy the ArcSight Manager's certificate you exported in [Step 8 on page 179](#) to your ArcSight Console's machine. You are required to import this certificate into the ArcSight Console's `nssdb.client` when installing the ArcSight Console.

To install the ArcSight 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 ArcSight Manager's certificate into the ArcSight Console's `nssdb.client`.

Run the following command to import the ArcSight Manager's certificate:



Note

If the machine on which you have installed the ArcSight Console is different than the ArcSight Manager machine, copy the ArcSight Manager's certificate you just exported on the ArcSight Manager machine to a pre-existing directory on the ArcSight Console machine before running the command below.

```
arcsight runcertutil -A -n ManagerCert -t "CT,C,C" -d
<ARCSIGHT_HOME>\current\config\nssdb.client -i
<absolute_path_to_ManagerCert.cer>
```



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. To check whether the certificate has been successfully imported, run the following from the ArcSight Console's `<ARCSIGHT_HOME>\bin` directory:

```
arcsight runcertutil -L -d
<ARCSIGHT_HOME>\current\config\nssdb.client
```

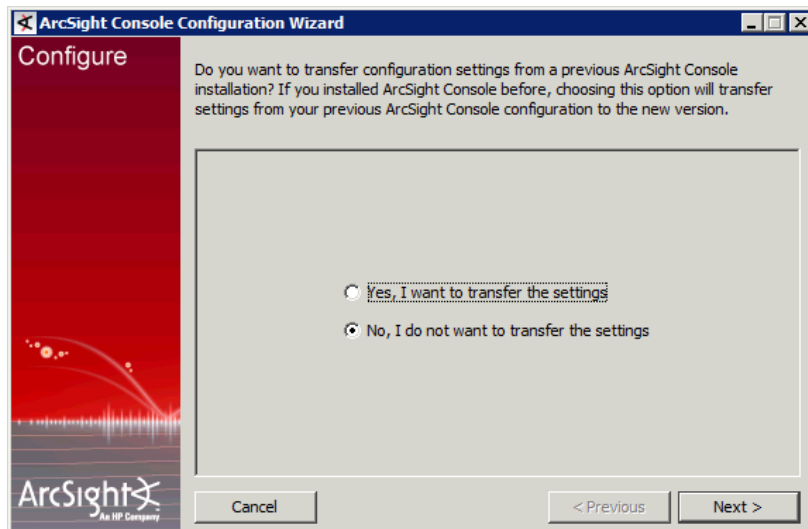


When you import or generate a key pair into NSS DB, if there is a existing key pair/certificate that has the same CN as the one you create, the `runcertutil` utility will use the existing alias for the newly created key pair and ignore the alias you supplied in the `runcertutil` command line.

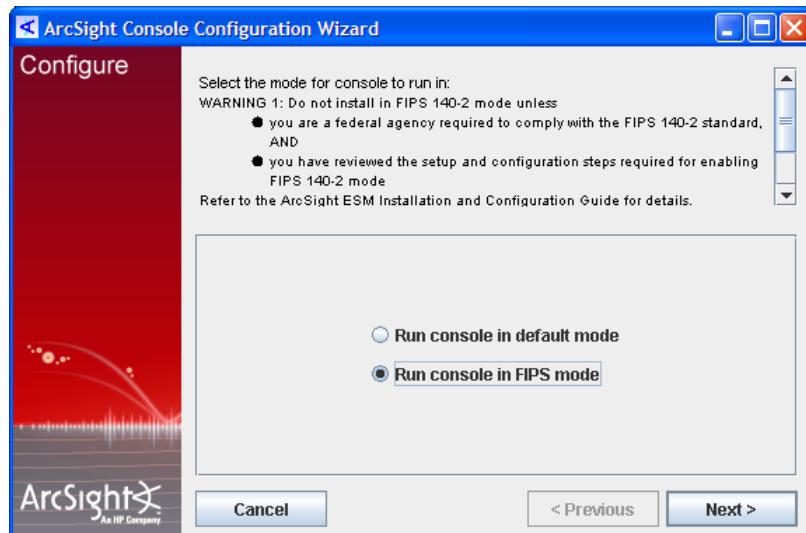
- 6 Go back to the wizard and select **No, I do not want to transfer the settings** in the following screen and click **Next**.

If you had exited the wizard after step 3, you can restart it by running the following command from the ArcSight Console's `bin` directory:

```
arcsight consolesetup
```

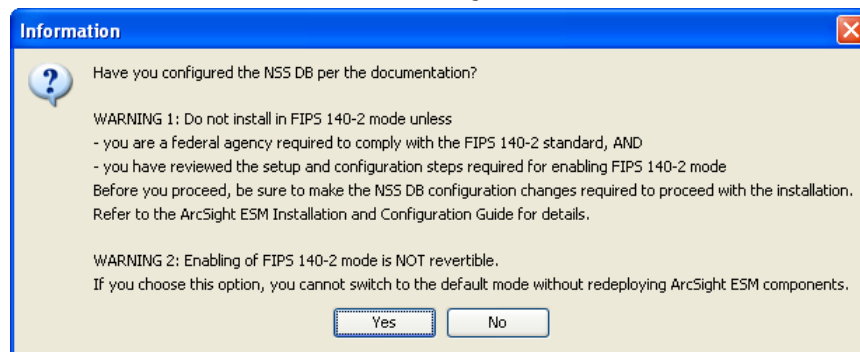


- 7 Next, you will see the following screen:

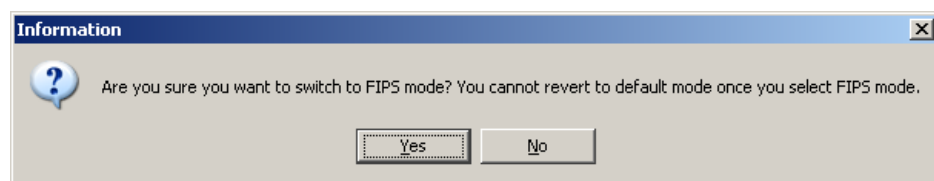


Select **Run console in FIPS mode** and click **Next**.

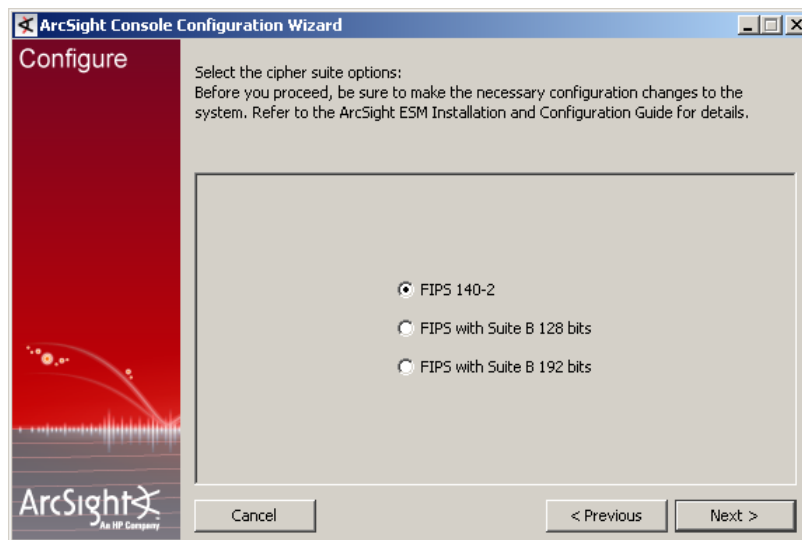
- 8 The configuration wizard will remind you to set up the NSS DB. Since you have already imported the ArcSight Manager's certificate into the ArcSight Console's `nssdb.client`, click **Yes** in the next dialog.



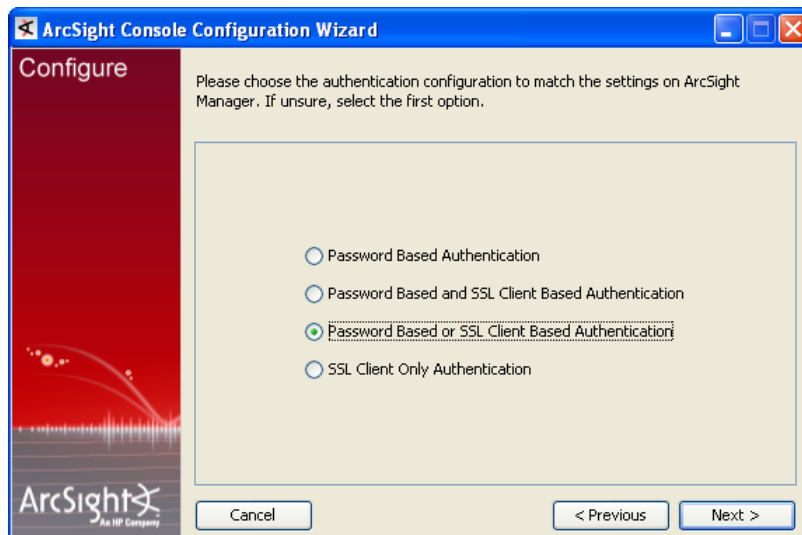
- 9 You will be reminded that once you select the FIPS mode, you will not be able to revert to the default mode. Click **Yes**.



- 10 You will be prompted to select a cipher suite. Select the type of FIPS the ArcSight Manager uses and click **Next**.



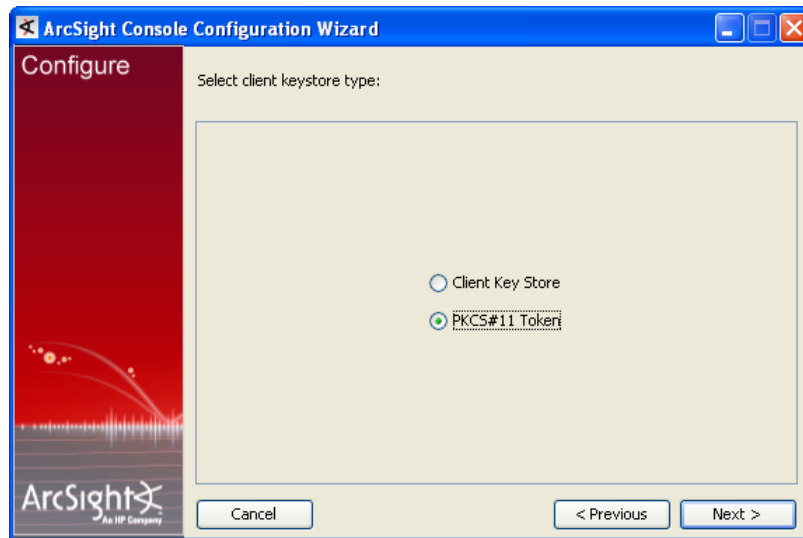
- 11 Next you will be prompted for the ArcSight Manager's hostname and port. The ArcSight Manager hostname must be the same (short name, fully qualified domain name, or IP address) as the Common Name (CN) you used when you created the ArcSight Manager key pair.
- 12 Follow the prompts in the next few wizard screens (Refer to the "Installing ArcSight Console" chapter, earlier in this guide, for details on any screen) until you get to the screen where you have to select the authentication option.



Select the option that you had set on the ArcSight Manager when installing it.

- 13 If you are using SSL client-based authentication and if you plan to use a PKCS #11 token with the ArcSight Console, select **PKCS #11 Token** option in the following

screen. If you are using different authentication, you do not see this screen and you can skip this step.



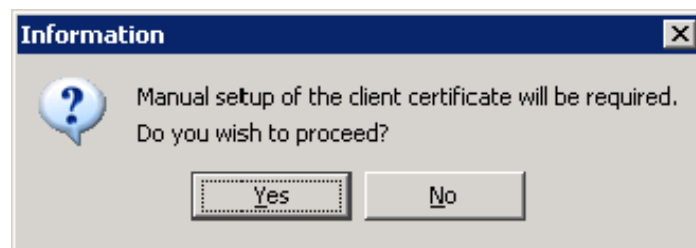
Enter the path or browse to the PKCS #11 library.

By default, the PKCS #11 library is located in the following directory:

On 64-bit Windows:

C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll  
(this is the 32-bit version of the ActivClient library)

If you do not plan to use a PKCS #11 token with the ArcSight Console, 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 in the topic “Setting up Client-Side Authentication,” in the “Configuration Changes Related to FIPS” appendix of the Administrator’s Guide.

- 14 Follow the prompts in the next few wizard screens to complete the ArcSight Console installation. Refer to the “Installing ArcSight Console” chapter, earlier in this guide, for details on any screen.



Note

If you have installed the product in FIPS with Suite B mode, select Firefox as your default browser when installing the ArcSight Console on Windows. You cannot use the Internet Explorer browser because it does not support FIPS with Suite B.

When you start the ArcSight Console, you should see a message saying that the ArcSight Console is being started in FIPS mode.

## Connecting a Default Mode ArcSight Console to a FIPS 140-2 ArcSight Manager

To have an ArcSight Console installed in the default mode to connect to a ArcSight Manager running in the FIPS 140-2 mode:

- Either add `server.fips.enabled=true` in your `console.properties` file located in the ArcSight Console's `<ARCSIGHT_HOME>\current\config` directory.  
Or add `-Dhttps.protocols=TLSv1` to the `ARCSIGHT_JVM_OPTIONS` variable in the ArcSight Console's `\current\bin\scripts\console.bat` file or `console.sh` file for Linux.
- Import the ArcSight Manager's certificate into `<ARCSIGHT_HOME>\current\jre\lib\security\cacerts` on the ArcSight Console using the `keytoolgui` tool. See section, "Using Keytoolgui to Import a Certificate" in the Administrator's Guide for details on how to do this.



Once you configure your ArcSight Console running in Default mode to connect to a FIPS enabled ArcSight Manager by following the steps above, you will not be able to connect this ArcSight Console to a ArcSight Manager running in Default mode without reversing the changes you made to the files.

---



You cannot connect a default mode ArcSight Console to an ArcSight Manager using FIPS Suite B.

---

## Connecting a FIPS ArcSight Console to FIPS Enabled ArcSight Managers

This procedure should be automatic for multiple ArcSight Managers. Just make sure that each ArcSight Manager certificate has a unique Common Name (CN) so that it's CN does not conflict with the CN of any existing certificate in the ArcSight Console's `nssdb.client`.

If you need to import a ArcSight Manager's certificate into the ArcSight Console's `nssdb.client` manually, refer to the Administrator's Guide for details on the procedure.

## 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 ArcSight Manager. We recommend installing ArcSight Web on a different machine than the ArcSight Manager.

If you choose to install the ArcSight Web on the same machine as the ArcSight Manager, when generating a key pair on the Web, set the CN for the ArcSight Web certificate to be the same as the CN that you used when generating the ArcSight Manager's certificate.

Install ArcSight Web only after you have installed the ArcSight Manager and have the ArcSight 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 ESM Product Lifecycle document available on the Protect 724 website for the most current information on supported platforms and web browsers.



Browsers that will be used to connect to ArcSight Web should be set to use the TLS v1 communication protocol. Currently, only Firefox is supported with Suite B. Refer to the ESM Product Lifecycle document available on the Protect 724 website for supported Firefox versions.

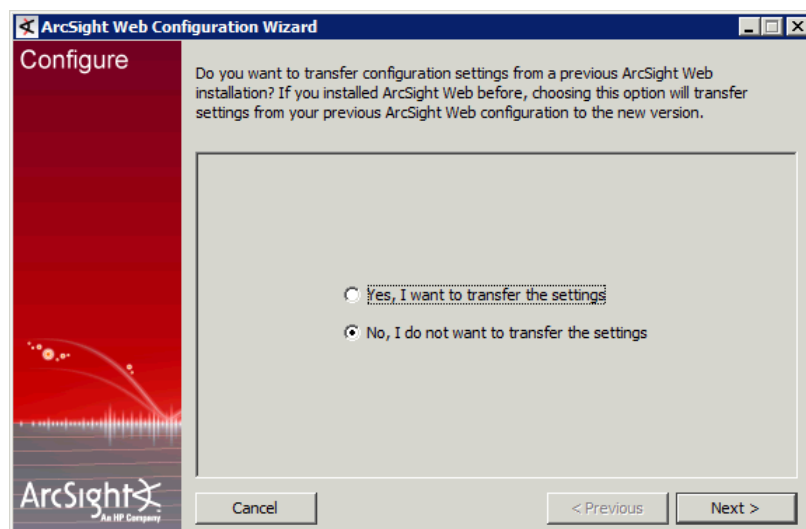
This section instructs you to install the Web in FIPS mode. For details on installing the Web in default mode, refer to the chapter, “[Installing ArcSight Web](#)” on page 129. The [Installing ArcSight Web](#) chapter also contains information that is common to both FIPS mode and default mode.

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 Administrator’s Guide for details on obtaining and using a CA-signed certificate.

The ArcSight Web exposes the ArcSight Manager’s services to the web browser. So, it acts as a server to the web browser but to the ArcSight Manager, it is a client. As a result, the Web setup is a combination of the ArcSight Manager setup and the client (ArcSight Console) setup. In other words, you have to generate a key pair on ArcSight Web (like you do on the ArcSight Manager) and also import the ArcSight Manager’s certificate into the webnsdb (like you do on the ArcSight 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 ArcSight Manager's certificate:

- a Run the following command to import the ArcSight Manager's certificate into ArcSight Web's webnssdb:



Note

If the machine on which you have installed the ArcSight Web is different than the ArcSight Manager machine, copy the ArcSight Manager's certificate you just exported on the ArcSight Manager machine to a pre-existing directory on the Web machine before running the command below.

```
./arcsight runcertutil -A -n <provide_an_alias_for_the_cert>
-t "CT,C,C" -d <ARCSIGHT_HOME>/config/jetty/webnssdb -i
<absolute_path_to_ManagerCert.cer>
```

```
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runcertutil -A -n ManagerCert -t
"CT,C,C" -d /home/arcsight/arcsight/Web-6391/config/jetty/webnssdb -i /home/arcsight/arcsight/Manager-6391/ManagerCert.cer

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight certutil starting...

arcsight:/home/arcsight/arcsight/Web-6391/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.

- b 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>
```



Caution

For the -t option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

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
```



Note

When you import or generate a key pair into webnssdb, if there is an 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 ArcSight Manager, the ArcSight 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 ArcSight 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`.



If you have installed ArcSight Web on the same machine as the ArcSight Manager, make sure to set the CN to be the same as the CN that you used when generating the ArcSight 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 Web's

`<ARCSIGHT_HOME>/config/jetty/webnssdb`.

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 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 Administrator's Guide for detailed steps on doing this.

- When you import or generate a key pair into `webnssdb`, if there is an 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`. Make sure that this serial number is different than the serial number that you had provided for the ArcSight Manager certificate when generating it.
- Using `-v` to set the validity period of your certificate is optional. If you do not use this option, the certificate will be valid for 3 months by default. If you choose to use it, see "Setting the Expiration Date of a Certificate" section in Administrator's Guide for details.
- For the `-t` option, be sure to use C,C,C protocols only.
- The hostname is the short name or fully qualified domain name depending upon how your ArcSight Web hostname was set up when you installed the ArcSight Manager.

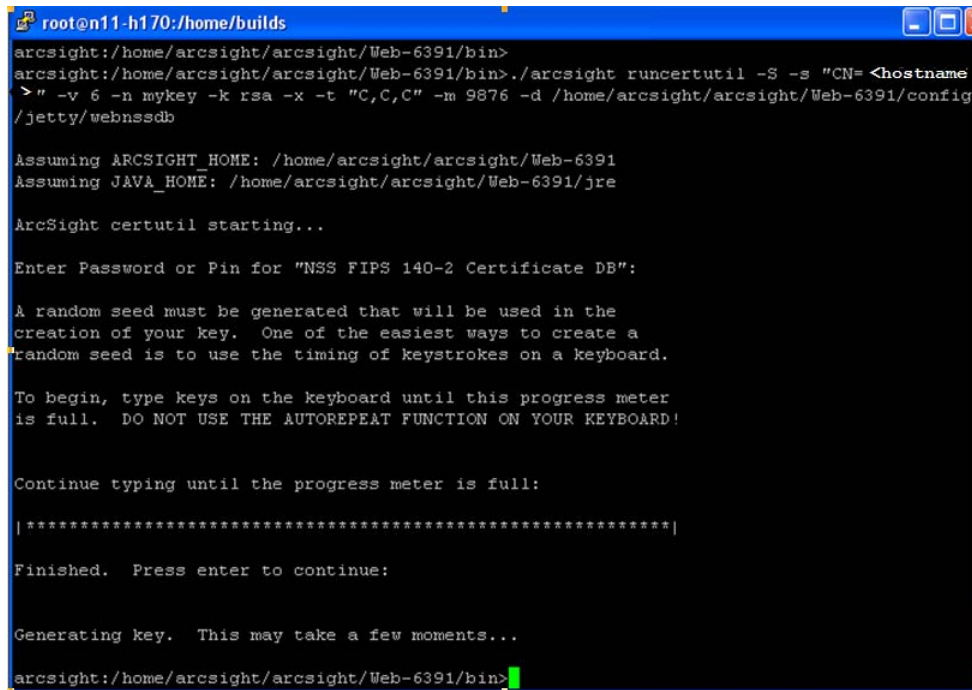
```
./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey
-k rsa -x -t "C,C,C" -m 9258 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

For example, if your hostname is `myhost.xyz.com`, you would run:

```
./arcsight runcertutil -S -s "CN=myhost.xyz.com" -v 6 -n
mykey -k rsa -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

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`

- 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.



```

root@n11-h170:/home/builds
arcsight:/home/arcsight/arcsight/Web-6391/bin>
arcsight:/home/arcsight/arcsight/Web-6391/bin>./arcsight runcertutil -S -s "CN= <hostname>" -v 6 -n mykey -k rsa -x -t "C,C,C" -m 9876 -d /home/arcsight/arcsight/Web-6391/config/jetty/webnssdb

Assuming ARCSIGHT_HOME: /home/arcsight/arcsight/Web-6391
Assuming JAVA_HOME: /home/arcsight/arcsight/Web-6391/jre

ArcSight 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...
arcsight:/home/arcsight/arcsight/Web-6391/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_HOME>/config/jetty/webnssdb
```

This command lists everything that is present in `webnssdb`. make sure that `mykey` is listed.

- 7 Go back to the wizard screen. Select **No, I do not want to transfer the settings** and click **Next**.

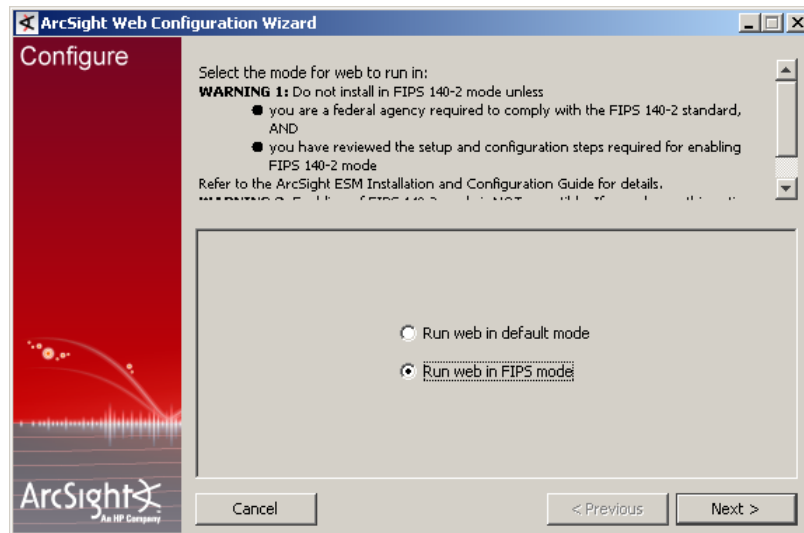


**Note**

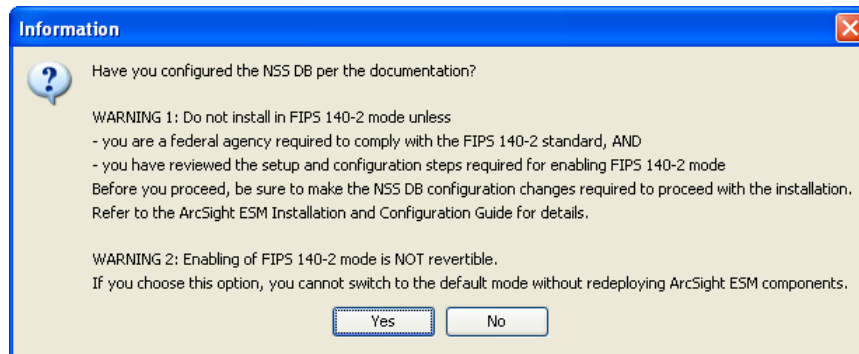
If you had exited the wizard after step 3, you can restart it by running the following command from the Web's `bin` directory:

```
arcsight webserversetup
```

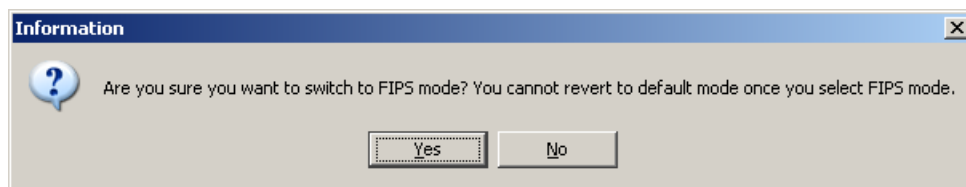
- 8 Select **Run web in FIPS mode** in the following screen and click **Next**:



- 9 You will see the following prompt asking you whether you configured your webnssdb. Since you have already imported the ArcSight Manager's certificate into the ArcSight Web's webnssdb and generated a keypair on the ArcSight Web, click **Yes**.

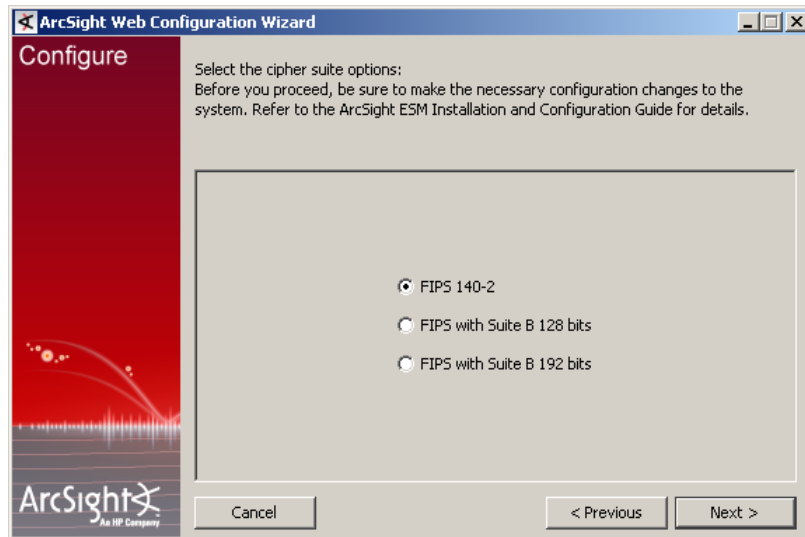


- 10 You will see the following warning:

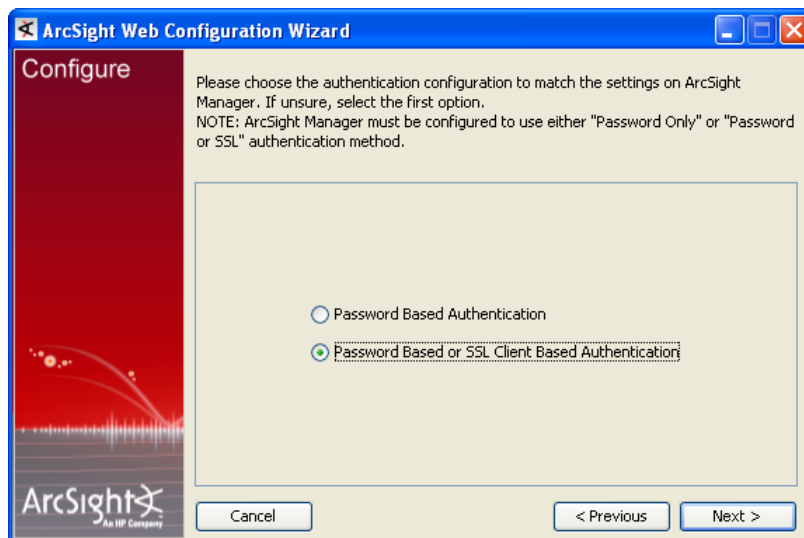


Click **Yes**.

- 11 You will be prompted to select a cipher suite. Select **FIPS 140-2** and click **Next**.



- 12 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 ArcSight Manager when installing it.

If you plan to use CAC with the Web, make sure to select **Password Based or SSL Client Based Authentication**.

- 13 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.
- 14 Start ArcSight Web by entering the following from ArcSight Web's `/bin` directory:

```
./arcsight webserver
```

Search for the "Ready" string in the `webserver.std.log` file to make sure that the webserver has started.

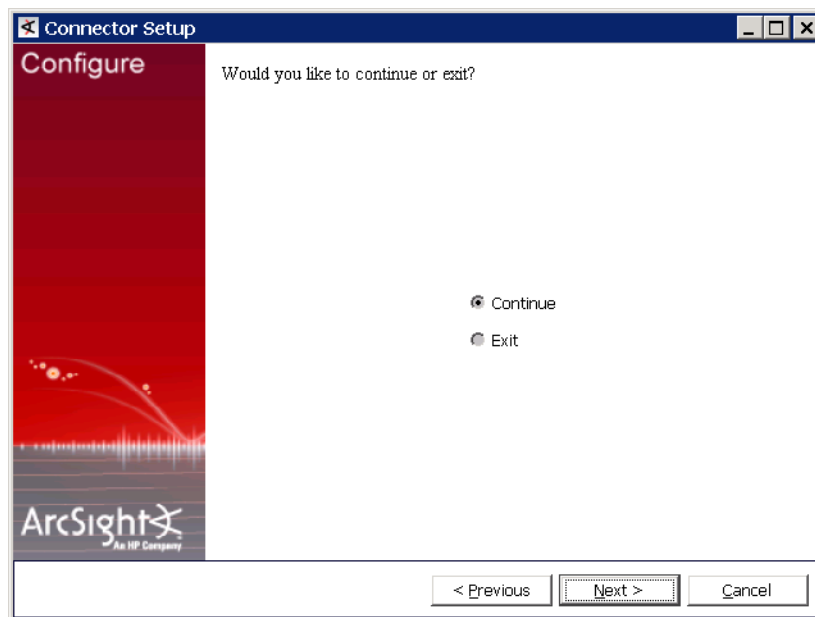
- 15 After you have completed installing ArcSight Web in FIPS mode, be sure you set your browser to use the TLS v1 communication protocol in order to make them FIPS compliant. Follow the procedures in your browser's documentation.

## Configure Your Browser for FIPS

To connect a browser to a FIPS web server, the browser must be configured to support FIPS. Review the documentation for your browser and follow the instructions to make it FIPS compliant before using it for ArcSight Console online help or to connect to .

## Installing SmartConnectors in FIPS mode

When the ArcSight Manager is installed in FIPS mode, the SmartConnectors must also be installed in FIPS mode. When you run the SmartConnector installation, continue until you see the screen below. Select **Continue** and click **Next**.



Use the following procedure to continue:

- 1 After choosing **Continue** and clicking **Next** after connector installation, choose **Enable FIPS Mode** and click **Next**. A confirmation window is displayed when FIPS mode is enabled.
- 2 Click **Next**. To complete installation of FIPS support, click **Exit**. To enable FIPS Suite B mode, click **Continue**.
- 3 On the window displayed, select **Modify Connector**.
- 4 Select **Add, Modify, or remove destinations** and click **Next**.
- 5 Select the destination for which you want to enable FIPS Suite B mode and click **Next**.
- 6 Select **Modify destination parameters** and click **Next**.
- 7 When the parameter window is displayed, select **FIPS with Suite B 128 bits** or **FIPS with Suite B 192 bits** for the **FIPS Cipher Suites** parameter. Click **Next**.

- 8 The window displayed shows the editing changes to be made. Confirm and click **Next** to continue. (To adjust changes before confirming, click **Previous**.)
- 9 A summary of the configuration changes made is displayed. Click **Next** to continue.
- 10 Click **Exit** to exit the configuration wizard.

For more information on installing SmartConnectors in FIPS mode see Installing FIPS-Compliant SmartConnectors. It is used in conjunction with the individual device SmartConnector configuration guides for your device.

## How do I Know if My 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 as follows:

- `<ARCSIGHT_HOME>\current\confi\gserver.properties` for the ArcSight Manager
- `<ARCSIGHT_HOME>\current\config\console.properties` for the ArcSight Console
- `<ARCSIGHT_HOME>\current\config\webserver.properties` for ArcSight Web
- `<ARCSIGHT_HOME>\user\agent\agent.properties` for the Partition Archiver. 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 `false`.

## Partition Archiver

To convert an existing Partition Archiver running in default mode to run in FIPS mode, you must import the ArcSight Manager's certificate and in case the ArcSight Manager uses a CA-signed certificate, the root certificate of the CA into the Partition Archiver's `nssdb.client`. To do so:

- 1 Export the ArcSight Manager's certificate by running the following command from the ArcSight Manager's `<ARCSIGHT_HOME>/bin` directory:

```
./arcsight runcertutil -L -n <certificate_alias> -r -d  
/config/jetty/nssdb -o <absolute_path_to  
_Manager's_certificate>
```

In case, the ArcSight Manager uses a CA-signed certificate, make sure to export the CA's root certificate from the ArcSight Manager.

- 2 Import ArcSight Manager's certificate (and the CA's root certificate in case of CA-signed certificate) into the Database's `usr/agent/nssdb.client` by running the following command from the Database's `bin` directory:

```
./arcsight runcertutil -A -n <manager_certificate_alias> -t  
"CT,C,C" -d /usr/agent/nssdb.client -i  
<absolute_path_to_the_manager's_certificate>
```

- 3 Run this command from the Database's `bin` directory:

```
./arcsight agentsetup
```

and follow the prompts on the screen to set up Partition Archiver in FIPS mode. Be sure to select the FIPS mode option when prompted for the mode in which to install.



## Appendix G

# Installing ESM in FIPS with Suite B Mode

---

This section covers the following topics:

- [“What is Suite B?” on page 201](#)
- [“Installing ArcSight Database” on page 202](#)
- [“Installing ESM in FIPS with Suite B Mode” on page 201](#)
- [“Setting up Partition Archiver in FIPS with Suite B” on page 208](#)
- [“Installing ArcSight Console in FIPS with Suite B Mode” on page 208](#)
- [“Installing ArcSight Web in FIPS with Suite B Mode” on page 208](#)
- [“Installing SmartConnectors in FIPS with Suite B Mode” on page 214](#)

This section provides you instructions for installing ESM in FIPS with Suite B mode.

To install ESM in default mode, follow the instructions in the respective chapters for installing the components.

To install ESM in FIPS mode (without Suite B), follow the instructions in [Appendix F, Installing ESM in FIPS Mode, on page 171](#).

Section [“Differences Between Default and FIPS Modes” on page 21](#) lists the basic differences between the three modes.



- Not all ESM versions or ArcSight Express models support the FIPS with Suite B mode. Refer to the ESM Product Lifecycle Document available on the Protect 724 website for supported platforms for FIPS with Suite B mode.
- When the Manager is installed in FIPS with Suite B compliant mode, the SmartConnectors must be installed in FIPS with Suite B compliant mode.
- ArcSight Web that connects to a Manager in FIPS with Suite B mode must also be installed in FIPS with Suite B mode.
- Before installing ESM in FIPS with Suite B mode, keep in mind that pre-v4.0 Loggers cannot communicate with a FIPS-enabled Manager.

## What is Suite B?

Suite B is a set of cryptographic algorithms put forth by the National Security Agency (NSA) as part of the national cryptographic technology. While FIPS 140-2 supports sensitive but

unclassified information, FIPS with Suite B supports both unclassified information and most classified up to top secret information. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.

When configured to use Suite B mode, ArcSight ESM supports Suite B Transitional profile. There are 2 level of security defined in Suite B mode:

- •TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA  
Suite B 128-bit security level, providing protection from unclassified to secret information
- •TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA  
Suite B 192-bit security level, providing protection from unclassified to top secret information

## Installing ArcSight Database

The steps to install ArcSight Database are the same regardless of the mode in which you want to install ESM. So, follow the instructions in the chapter, [“Installing ArcSight Database” on page 33](#) to install the Database.

## Installing ArcSight Manager in FIPS with Suite B Mode

ArcSight Manager requires that the ArcSight Database be installed first.

This section instructs you on installing the Manager in FIPS with Suite B mode only. The [Installing ArcSight Manager](#) chapter lists the supported platforms for ArcSight Manager and contains information that is common to FIPS mode, FIPS with Suite B mode, and default mode. You can also refer to the ArcSight ESM Product Lifecycle document available on the Protect 724 website for supported platforms.



**Note**

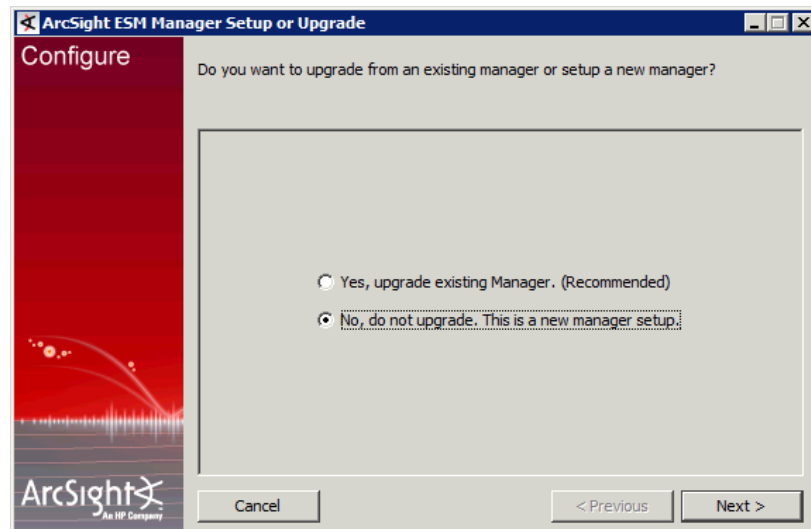
For detailed information on any of the utilities in this chapter, refer to “Appendix A, ArcSight Commands” in the *Administrator’s Guide*.

---

To install the Manager in FIPS with Suite B mode:

- 1 Create an ArcSight user 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.
- 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 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**

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 uses the alias of the existing key pair for the newly created key pair and ignores 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 automatically generates 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
- The hostname is the short name or fully qualified domain name depending upon how your ESM manager name was set up when you installed the Manager.
- Using -v to set the validity period of your certificate is optional. If you do not use this option, the certificate is valid for 3 months by default. If you choose to use it, see ["Setting the Expiration Date of a Certificate" on page 213](#) section in the *ArcSight ESM Administrator's Guide* for details.
- The -q defines the PQG value with which an ECDSA certificate is generated.

```
./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey
-k ec -q secp521r1 -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/nssdb
```

For example, if your hostname is host.arcsight.com, you would run:

```
./arcsight runcertutil -S -s "CN=host.arcsight.com" -v 6 -n
mykey -k ec -q secp521r1 -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/nssdb
```

When prompted for password, enter "changeit" (without the quotes).

Enter random keyboard strokes when prompted to generate a random seed, used to generate your key.

This generates a key pair and certificate with the alias `mykey` that is valid for six months from the current date and time in the Manager's `nssdb`.

- 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
```

**8** Export the Manager's certificate.

Have this exported certificate handy when installing the clients (Console and/or Web) that connects to this Manager. Import this certificate into the clients' NSS DB (`<ARCSIGHT_HOME>/current/config/nssdb.client` for the Console and `<ARCSIGHT_HOME>/config/jetty/webnssdb` for 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>
```



The -o specifies the absolute path to the location where you want the exported Manager's certificate to be placed. If you do not specify the absolute path, the export function exports the certificate to your <ARCSIGHT\_HOME> directory by default.

For example, to export the certificate as a file named ManagerCert.cer to C:\arcsight\Manager directory, run:

```
./arcsight runcertutil -L -n mykey -r -d
<ARCSIGHT_HOME>/config/jetty/nssdb -o
/home/arcsight/arcsight/Manager-6391/ManagerCert.cer
```

This command generates the ManagerCert.cer file, the Manager's certificate, in the /home/arcsight/arcsight/Manager-6391 directory.

#### 9 (Only if you plan to use CAC with this ESM setup)

If you plan to use CAC with the Console or Web, import the CAC card's CA's root certificate into the Manager's nssdb. See the sections [“Obtain the CAC's Issuers' Certificate” on page 218](#) and [“Extract the Root CA Certificate From the CAC Certificate” on page 220](#) for details on how to obtain the CAC card's CA's root certificate.

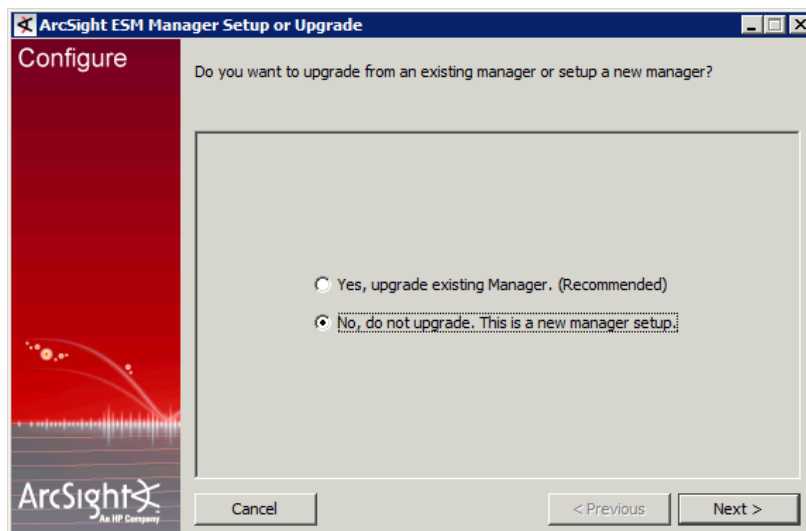
To import the CAC card's CA's root certificate into the Manager run:

```
./arcsight runcertutil -A -n CACcert -t "CT,C,C" -d
<ARCSIGHT_HOME>/config/jetty/nssdb -i
<absolute_path_to_the_root_certificate>
```

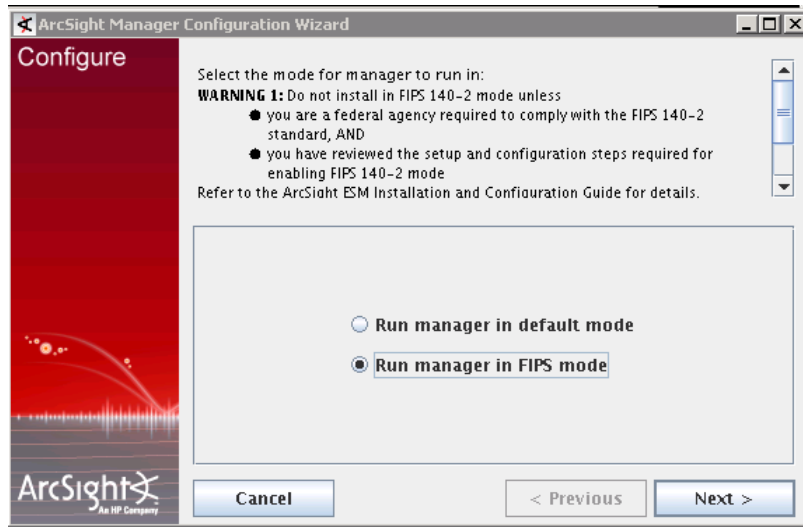


For the -t option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- 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**.

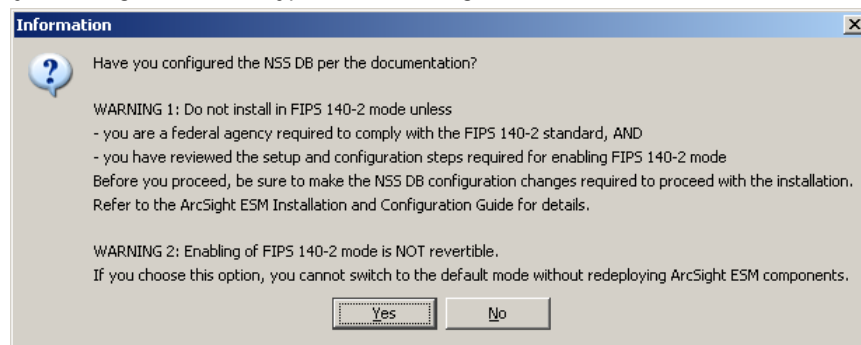


- 11 Next, you see the following screen:

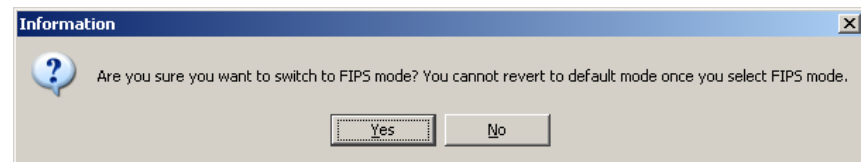


Select the **Run manager in FIPS mode** radio button and click **Next**.

- 12 The configuration wizard asks you to confirm that you have set up the NSS DB. Since you have generated a keypair in the Manager's NSS DB, click **Yes**.

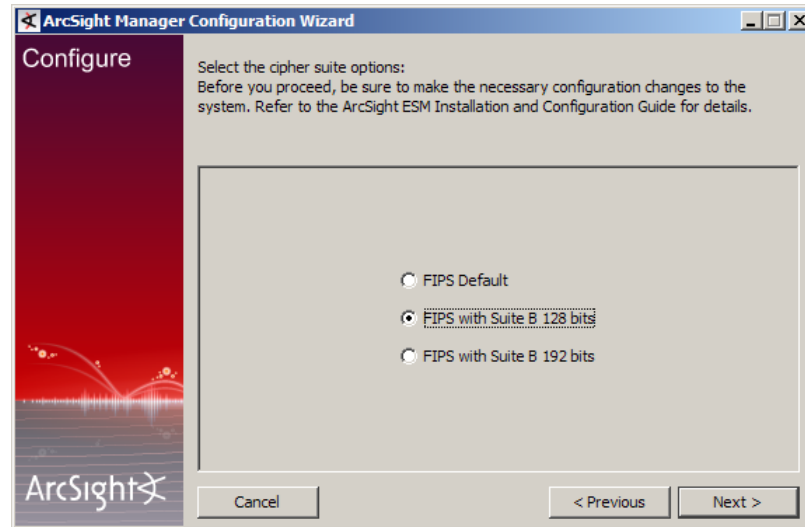


- 13 You are reminded that once you select FIPS mode, you cannot revert to default mode. Click **Yes**.

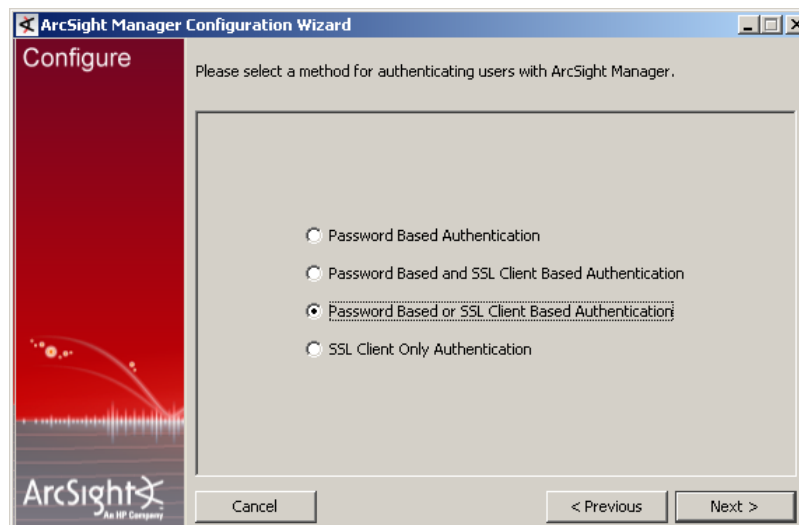


- 14 Suite B defines two security levels of 128 and 192 bits. The two security levels are based on the Advanced Encryption Standard (AES) key size that is used instead of the overall security provided by Suite B. At the 128-bit security level, the 128 bit AES key size is used. However, at the 192-bit security level, a 256 bit AES key size is used. Although, a larger key size would mean more security, it would also mean computational cost in terms of time and resource (CPU) consumption. In most scenarios, the 128-bit key size is sufficient.

Select the **FIPS with Suite B 128 bits** option in the following screen:



- 15 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 (no Web):  
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:  
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.

- 16 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.
- 17 Start the ArcSight Manager by entering the following from the Manager's `/bin` directory:

```
./arcsight manager
```

When the Manager starts up, it displays a stream of messages in the terminal window to reflect its status.

## Setting up Partition Archiver in FIPS with Suite B

After the ArcSight Manager has been installed and running, you can optionally configure the Partition Archiver on the ArcSight Database host.

Follow the section [“Setting up Partition Archiver in FIPS Mode” on page 183](#) for installing the Partition Archiver. The steps to install Partition Archiver in FIPS with Suite B mode are identical to the steps for installing Partition Archiver in FIPS mode.

While setting up Partition Archiver in Suite B mode, the setup wizard might fail with a pop-up error dialog. To resolve this problem:

- 1 Close this error dialog and click Cancel to exit the agent setup wizard.
- 2 Create or edit the `<ARCSIGHT_HOME>/user/agent/agent.properties` file and add the following line to this file:

```
fips.enabled=true
```

- 3 Run `arcsight agentsetup` again to register the Partition Archiver.

## Installing ArcSight Console in FIPS with Suite B Mode

Install and test the ArcSight Database and Manager before installing the ArcSight Console. Follow the section [“Installing ArcSight Console in FIPS Mode” on page 184](#) for installing the Console. The steps to install the Console in FIPS with Suite B mode are identical to the steps for installing the Console in FIPS mode.



Note

Make sure to select the Firefox browser when installing ESM in Suite B mode. Internet Explorer browser is not supported.

---

## Installing ArcSight Web in FIPS with Suite B 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 Protect 724 website for the most current information on supported platforms and web browsers.

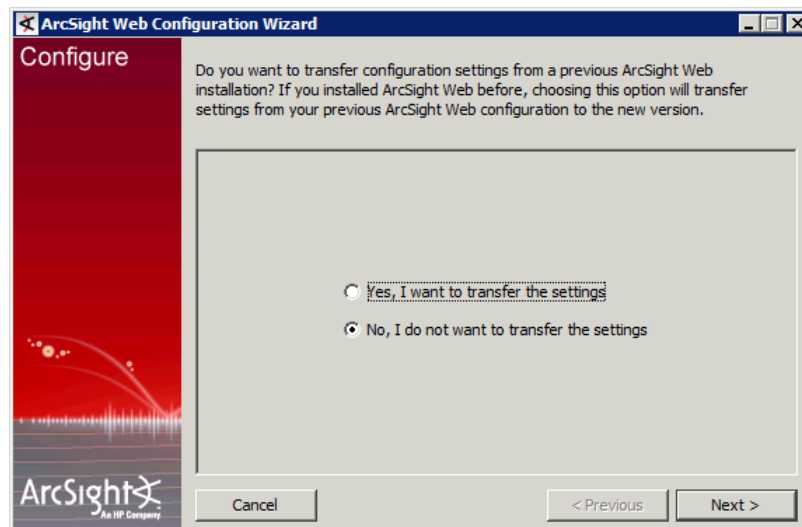


Set browsers that you use to connect to ArcSight Web to use the TLS v1 communication protocol. Currently, only Firefox is supported with Suite B. Follow instructions in the section [“Configure Your Browser for FIPS” on page 197](#) for details on configuring Firefox in order to use it with your Suite B installation.

Refer to the ArcSight ESM Product Lifecycle document available on the Protect 724 website for supported Firefox versions.

To install and configure ArcSight Web in FIPS with Suite B mode:

- 1 Stop ArcSight Web if it is running.
- 2 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.
- 3 Follow the prompts in the wizard screens. Refer to [Installing ArcSight Web](#) chapter for details on any screen.
- 4 When you get to the first configuration screen as shown below, leave the wizard running:



- 5 Open a shell window.
- 6 Import the Manager's certificate:
  - a 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_ManagerCert.cer>
```



For the -t option, be sure to use CT,C,C protocols only and in the same order that it is shown above.

- b Skip this step if you do not use CAC with ArcSight Web. Go to [Step 7](#).

**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.

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
```



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 uses the alias of the existing key pair/certificate for the newly created key pair and ignores 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 has the same CN as the key pair you generated for ArcSight Web. Hence, the runcertutil utility uses the same alias for the Manager's certificate and the Web's key pair that you generated.

- 7 Generate a key pair on the Web server with an alias mykey. This automatically generates the key pair and the Web's certificate in the webnssdb:.



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.

**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 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.

- a** Run the following command from the Web's `<ARCSIGHT_HOME>/bin` directory to generate a key pair. This automatically generates 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`. Make sure that this serial number is different than the serial number that you had provided for the Manager certificate when generating it.
- Using `-v` to set the validity period of your certificate is optional. If you do not use `-v` to specify a validity period for the certificate, the certificate is valid for three months by default. If you choose to use it, see "Setting the Expiration Date of a Certificate" section in ArcSight ESM Administrator's Guide for details.
- For the `-t` option, be sure to use `C,C,C` protocols only.
- The hostname is the short name or fully qualified domain name depending upon how your ArcSight Web host name was set up when you installed the Manager.

```
./arcsight runcertutil -S -s "CN=<hostname>" -v
<number_of_months_the_certificate_should_be_valid> -n mykey
-k ec -q secp521r1 -x -t "C,C,C" -m 9258 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

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 ec -q secp521r1 -x -t "C,C,C" -m 1234 -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

- 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, used to generate your key.

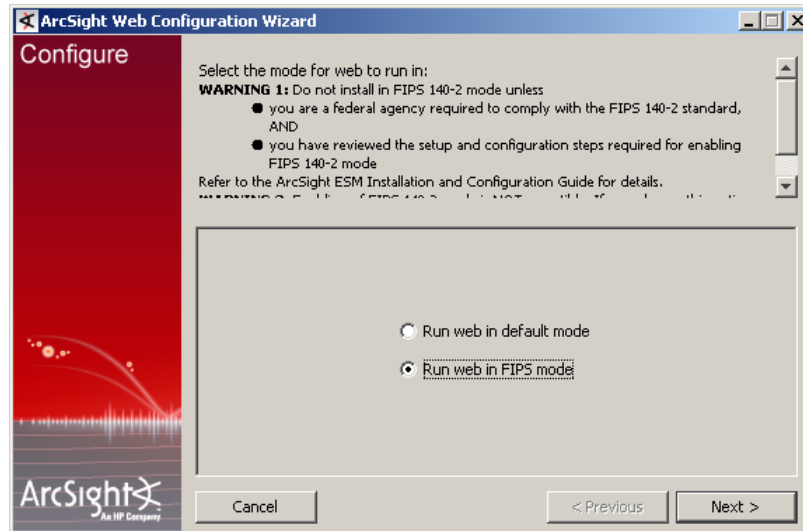
This generates a key pair and certificate with the alias `mykey` that is valid for 6 months from the current date and time in the Web's `webnssdb`.

To check whether the key pair has been successfully created in the `webnssdb`, run the following from ArcSight Web's `<ARCSIGHT_HOME>/bin` directory:

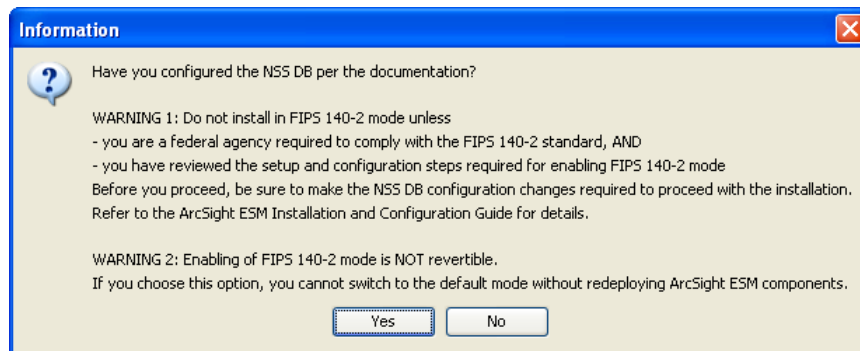
```
./arcsight runcertutil -L -d
<ARCSIGHT_HOME>/config/jetty/webnssdb
```

This command lists the contents of the webnssdb. Check to make sure that mykey appears in the list.

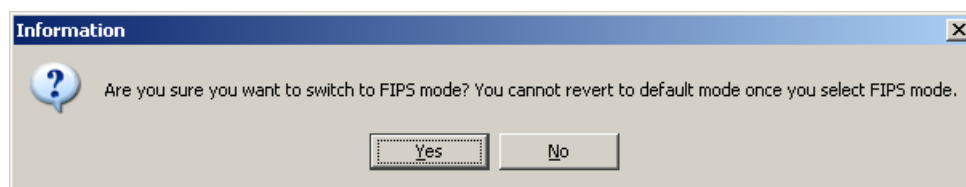
- 8 Go back to the wizard screen. Select **No, I do not want to transfer the settings** and click **Next**.
- 9 Select **Run web in FIPS mode** in the following screen and click **Next**:



- 10 You see the following prompt asking you whether you configured your webnssdb. Since you have already imported the Manager's certificate into the Web's NSS DB and also generated the Web's keypair, click **Yes**.

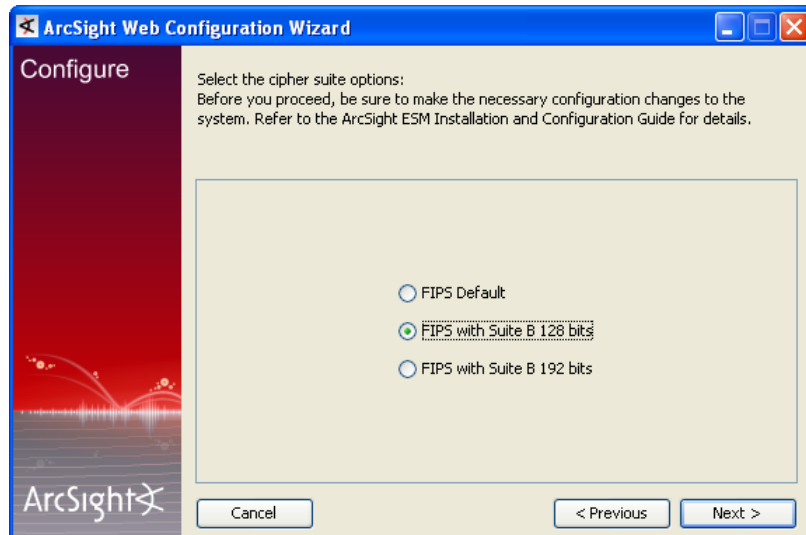


- 11 You get the following dialog:



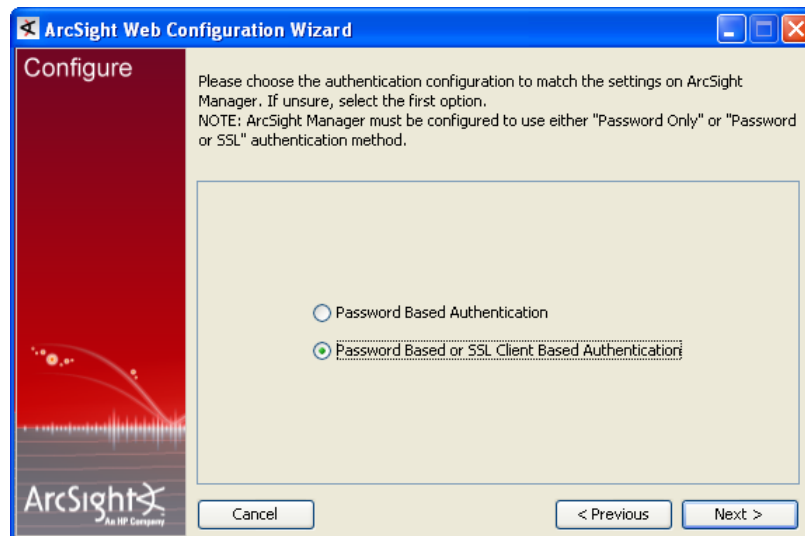
Click **Yes**.

- 12 Next you are prompted to select a key size.



Select **FIPS with Suite B 128 bits**.

- 13 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**.

- 14 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.
- 15 Start ArcSight Web by entering the following from ArcSight Web's `/bin` directory:
- ```
./arcsight webserver
```
- 16 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 ["Configure Your Browser for FIPS" on page 197](#).

## Installing SmartConnectors in FIPS with Suite B Mode

When the Manager is installed in FIPS with Suite B compliant mode, the SmartConnectors must also be installed in FIPS with Suite B compliant mode.

See the Installing FIPS-Compliant SmartConnectors Guide for information on installing SmartConnectors in FIPS mode. Additional configuration is required to run the connector in FIPS with Suite B compliant mode. Follow the instructions in "Enable FIPS Suite B Support" in the SmartConnector Configuration Guide for your connector, following "SmartConnector Installation" and preceding "Run the Connector."

## Appendix H

# Using the PKCS#11 Token

---

This appendix covers the following topics:

- ["What is PKCS?" on page 215](#)
- ["PKCS#11 Token Support in ESM" on page 216](#)
- ["Setting Up to Use a CAC Card" on page 216](#)
- ["Using CAC with ArcSight Web" on page 225](#)

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 ArcSight Manager is running in - with ArcSight Manager running in FIPS 140-2 mode or with ArcSight Manager running in the default mode.
- PKCS #11 token support may not be available for all ESM versions and ESM models. Refer to the ESM Product Lifecycle Document available on the Protect 724 website for information on supported platforms for PKCS #11 Token.

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

## What is PKCS?

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

## PKCS#11

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

## PKCS#12

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

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 ArcSight Console and ArcSight Web systems 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 (FIPS 140-2 mode or default mode).

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

## Setting Up to Use a CAC Card

Even though ESM supports authentication through any PKCS#11 token, this appendix covers how to use the ActivClient's Common Access Card (CAC) as an example.

### Install the CAC Provider's Software

Before you use the Common Access Card (CAC), make sure that you have installed its software on each client system. That includes the ArcSight Console and any machine with a browser from which you intend to access the Management Console. Refer to your CAC provider's documentation on how to install and configure it.



Install both the 32-bit version and the 64-bit version of the ActivClient software if you are on a 64-bit system. You can do so by double-clicking on the `setup.exe` link instead of the `.msi` files for the specific platform.

---

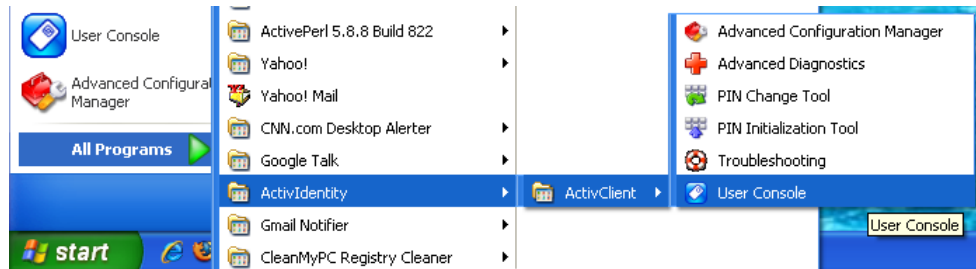
### Map a User's External ID to the CAC's Subject CN

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

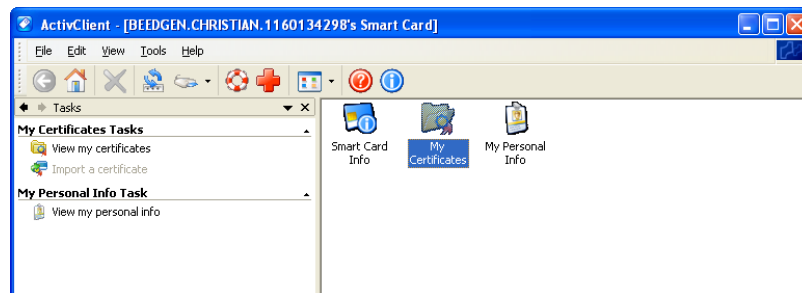
Map the Common Name (CN) on the CAC to a User's External ID on the ArcSight Manager. The external user ID must be identical to the Common Name that appears in the CAC card's ID certificate (include any spaces and periods that appear in the Common name). This allows the ArcSight Manager to know which user is represented by the identity stored in the CAC card.

You can do this in the Management Console's **Admin** tab under User Management, when adding or editing a user.

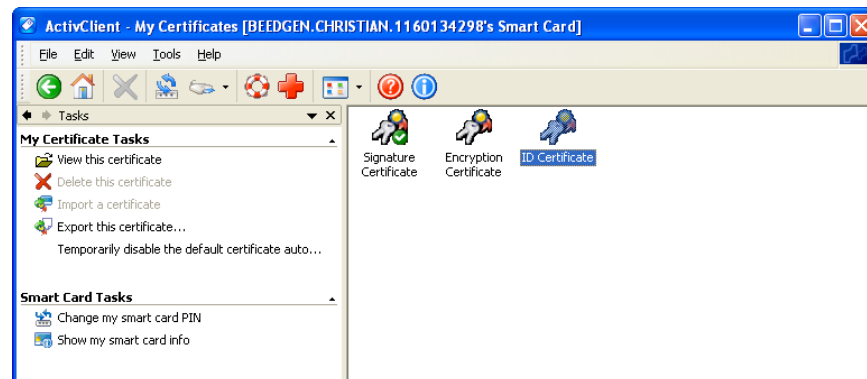
- 1 Obtain the Subject CN from the CAC card.
  - a Insert the CAC card into the reader if not already inserted.
  - b Start the ActivClient Software by clicking **Start > ActivIdentity > ActivClient > User Console**.



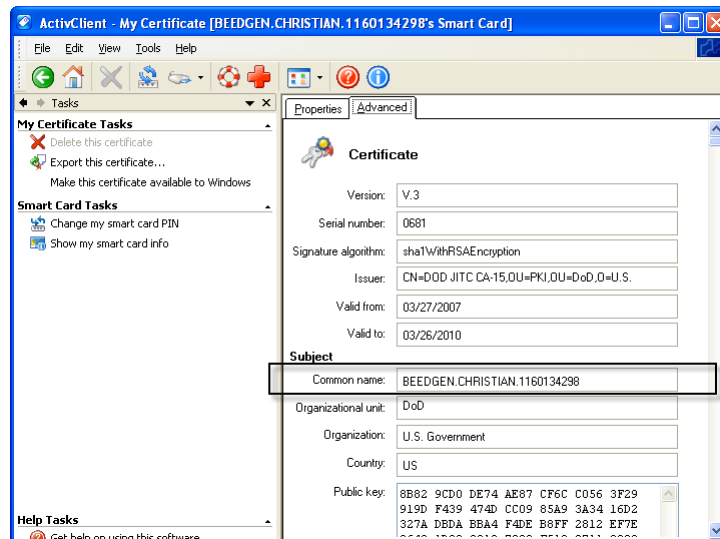
- c Double-click **My Certificates** in the following screen:



- 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 the Management Console, go to the **Administration** tab to edit the user to make the external ID match the CN.
  - a Select **User Management**, on the left.
  - b In the hierarchy tree on the left, click on the group containing the user.
  - c To edit a user, click anywhere on the user's row in the list. The user details fields appear in the lower half of the list.
  - d In the External ID field, enter the CN you obtained in step 1 and click **Save**. It must be identical, character by character.

Alternately, you can make the external ID match the CN in the ArcSight Console:

- a In the ArcSight Console, go to **Resources > Users > [user group]** and double-click the user whose External ID you want to map to the CAC card common name. This opens the Inspect/Edit pane for that user.
- b Enter the CN you obtained in step 1 into the **External User ID** field and click **Apply**.

## Obtain the CAC's Issuers' 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 keystore so that you can extract the root CA and any intermediate certificates from this certificate.

If your certificate is issued by an intermediate CA, export not only the issuer (the intermediate root CA) certificate, but also, its top root CA certificate.

### Option 1:

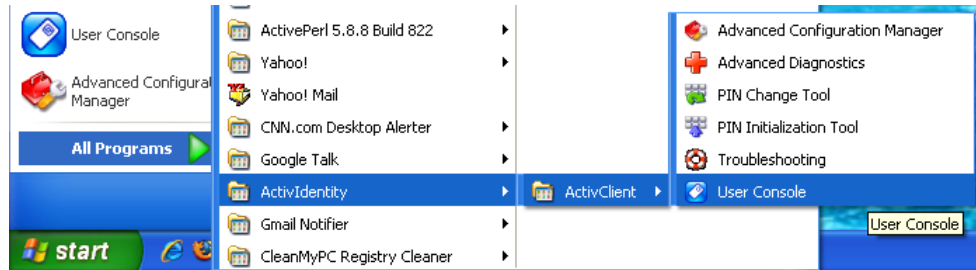
You can obtain the CAC card's certificate signer's root CA certificate and any intermediate signers' certificates from the PKI administrator.

### Option 2:

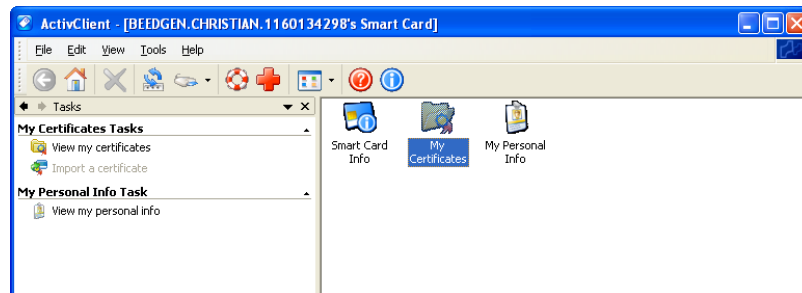
You can export the CAC card's certificate and any intermediate signers' certificates from its keystore and then extract the root CA certificate from this certificate.

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

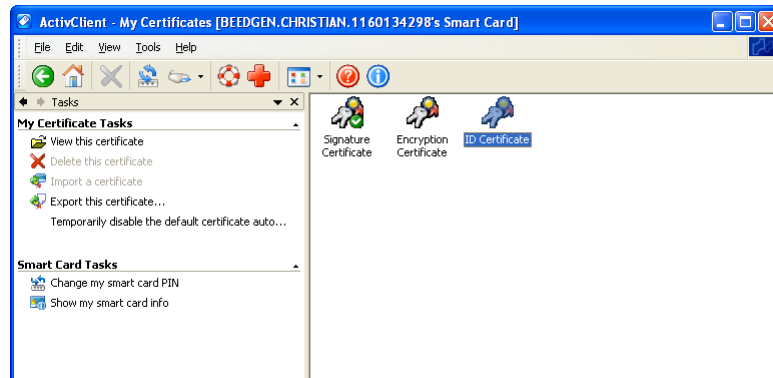
- 1 Insert the CAC card into the reader if not already inserted.
- 2 Start the ActivClient Software by clicking **Start->ActivIdentity->ActivClient->User Console**.



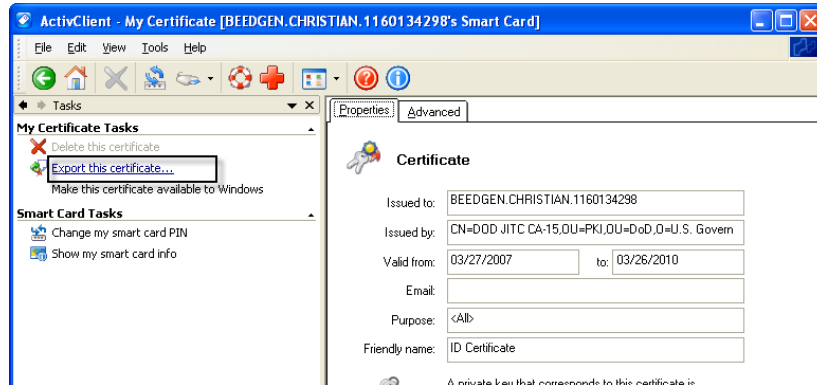
- 3 Double click **My Certificates** in the following screen:



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



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



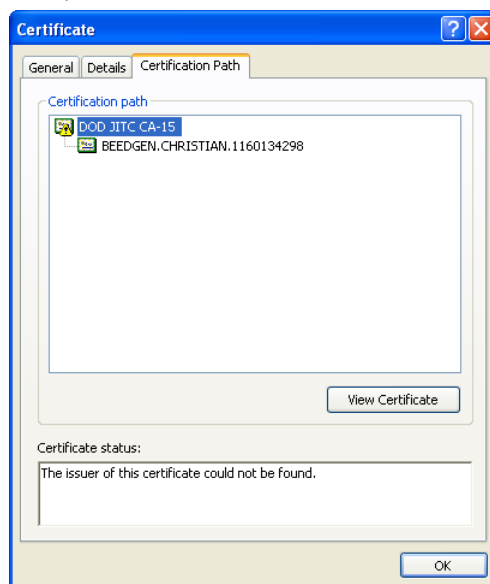
- 6 Enter a name for the certificate in the **File name** box and navigate to a location on your machine where you want to export it to and click **Save**.
- 7 When you see the success message, click OK.
- 8 Exit the ActivClient window.

## Extract the Root CA Certificate From the CAC Certificate

The CAC certificate signer's CA root certificate and any intermediate signers' certificate(s) have to be imported into the ArcSight Manager's `nssdb` (in FIPS mode) or `truststore` (in default mode) and if you are planning to use CAC with ArcSight Web, Web's `webnssdb` (in FIPS mode) or `truststore` (in default mode).

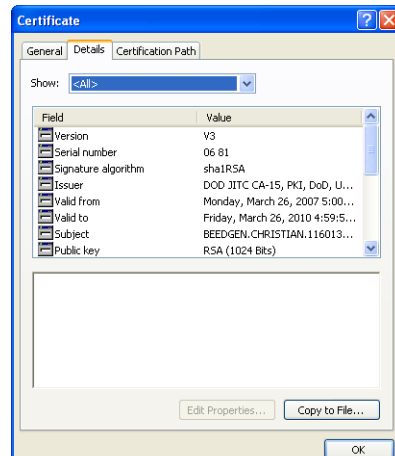
Extract all intermediate certificates too (if any exist) using the following steps:

- 1 Double-click the CAC's certificate that you exported. The Certificate interface opens.
- 2 Click the **Certification Path** tab and select the root certificate as shown in the example below:



- 3 Click **View Certificate**.

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



- The Certificate Export Wizard opens. Follow the prompts in the wizard screens and accept all the defaults.
- Enter a name for the CAC root CA certificate file when prompted and continue with the wizard by accepting all the defaults. The certificate is exported to the same location as the CAC certificate from which you extracted it.
- Exit the Certificate dialog.

## Import the CAC Root CA Certificate into the ArcSight Manager

This procedure is slightly different depending on whether you are in FIPS or default mode:

### FIPS Mode - Import into the ArcSight Manager's nssdb

To import the certificate into the ArcSight Manager's nssdb:

- If the Arcsight Manager is running, log in as user *arcsight* (see ["About the ArcSight User" on page 83](#)). Then use this command:

```
/etc/init.d/arcsight_services stop manager
```

- Import the CAC card signer's CA 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.

- Restart the ArcSight Manager while logged in as user *arcsight* by running:

```
/etc/init.d/arcsight_services start manager
```

### Default Mode - Import into ArcSight Manager's Truststore

Use the following procedure to import the CAC card's root CA certificate into the ArcSight Manager' truststore:

- 1 Start the keytoolgui command from the component into which you want to import the certificate. To do so, run the following command from the component's `/bin` directory.

```
./arcsight keytoolgui
```

- 2 Click **File->Open keystore** and navigate to the truststore directory (`<ARCSIGHT_HOME>/config/jetty/truststore`) of the Manager.
- 3 Select the store named `truststore` and click **Open**.
- 4 Enter the password for the truststore when prompted. The default password is *changeit*.
- 5 Click **Tools->Import Trusted Certificate** and navigate to the location of the certificate that you want to import.
- 6 Click **Import**.
- 7 When you see the message that the certificate information will be displayed, click **OK**.
- 8 The Certificate details are displayed. Click **OK**.
- 9 When asked if you want to accept the certificate as trusted, click **Yes**.
- 10 Enter an alias for the Trusted Certificate you just imported and click **OK**.
- 11 When you see the message that the import was successful, click **OK**.
- 12 Save the truststore file.
- 13 As user *arcsight*, restart the ArcSight Manager by running:

```
/etc/init.d/arcsight_services start manager
```

## Select Authentication Option in managersetup

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



### Caution

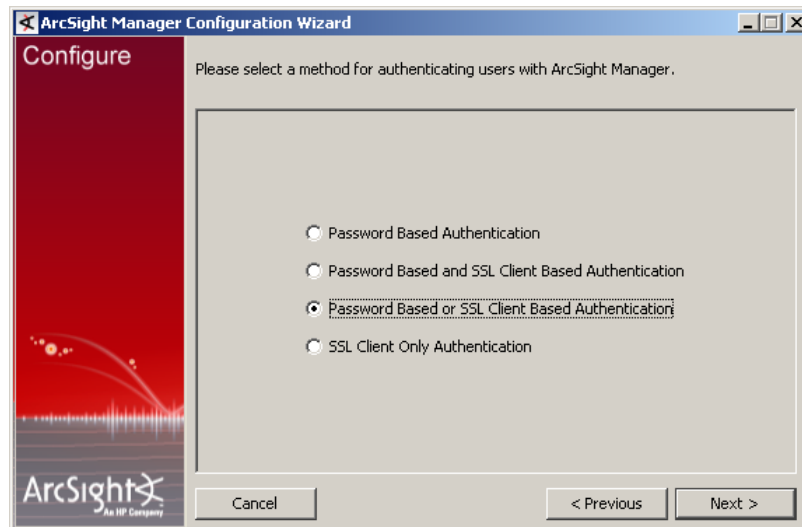
The authentication option you select on the ArcSight Manager has to match the authentication option on ArcSight Web.

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

To set the authentication option on the ArcSight Manager:

- 1 Run the ArcSight Manager's setup program from the ArcSight 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 ArcSight Manager.

## Select Authentication Option in ArcSight Console Setup

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

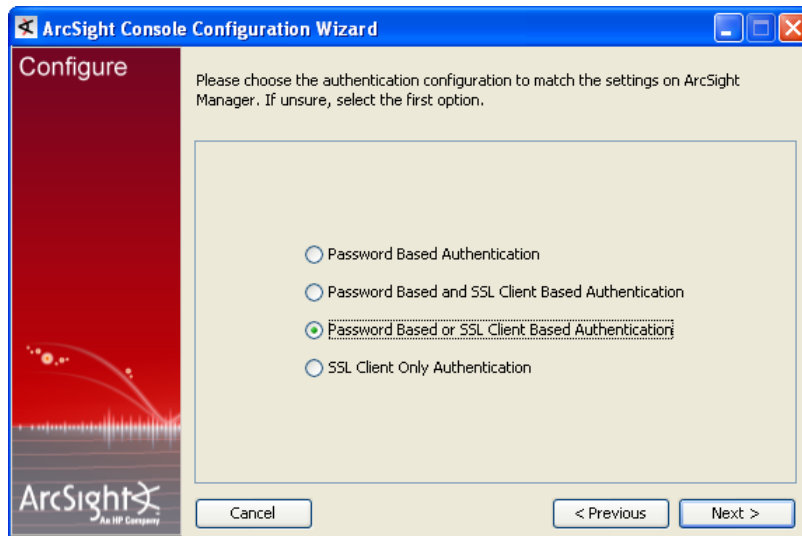
- 1 Stop the ArcSight Console if it is running.
- 2 Run the ArcSight Console's setup program from the ArcSight Console's bin directory:  

```
arcsight consolesetup (Windows)
```

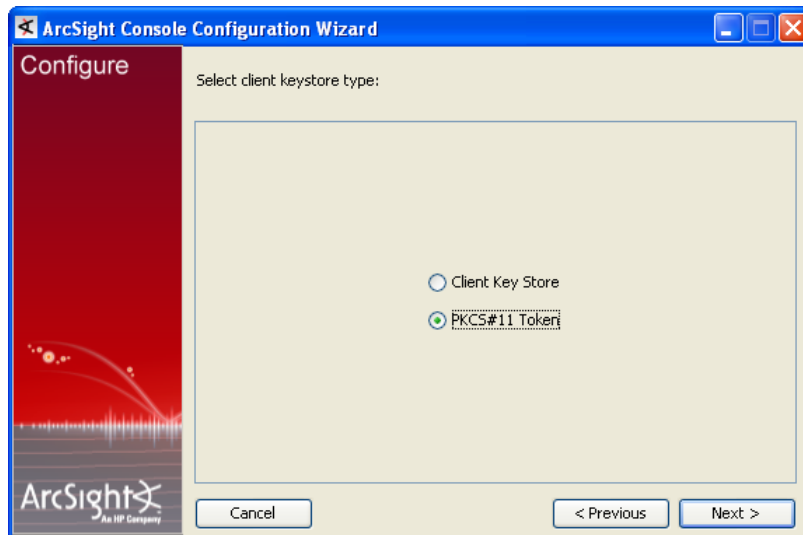
  

```
./arcsight consolesetup (Linux)
```
- 3 Follow the prompts in the wizard screens by accepting all the defaults until you see the screen for the authentication option shown in the next step.

- 4 Select the authentication that you selected for the ArcSight 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 when prompted.

By default on 32-bit Windows platforms PKCS#11 dll could be found in  
C:\Windows\System32.

If you are using a vendor other than ActivClient, this should point to the library location for that installation.

If you are using ActiveClient, by default the PKCS #11 library is located in:

On 32-bit Windows:

C:\Program Files\ActivIdentity\ActivClient\acpkcs211.dll

On 64-bit Windows:

C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll  
(this is the 32-bit version of the ActivClient library)

- 8 Complete the setup program by accepting all the defaults.
- 9 Restart any running ArcSight Consoles.

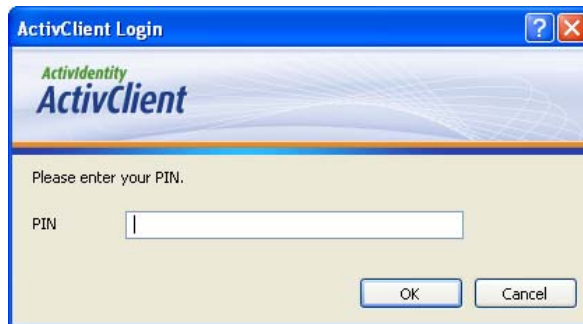
## Logging in to the ArcSight Console Using CAC

When you start the ArcSight Console, you will see a screen with a PKCS #11 login button.

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

- Username and password combination (For this option, disconnect the CAC card.)
- PKCS#11 Login

To log in using CAC, select the PKCS #11 Login option. In the following dialog, enter the PIN number of your ActivClient card in the **PIN** text box.



If you plan to use Internet Explorer, configure it to be FIPS compliant.

## Using CAC with ArcSight Web

To use CAC with ArcSight Web:

- 1 Export the CAC's certificate. You have two options to do this.

### Option 1:

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

### Option 2:

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

- a To export the CAC card's certificate, follow the instructions in ["Obtain the CAC's Issuers' Certificate" on page 218](#) for details. Make sure that this certificate is available on the system on which you have installed ArcSight Web.
  - b Extract the CA's root certificate from the CAC certificate. See ["Extract the Root CA Certificate From the CAC Certificate" on page 220](#) for details.
- 2 Stop ArcSight Web if it is running.
  - 3 Import the CAC Card Signer's Root CA Certificate.

### FIPS Mode:

To import the certificate into the Web's `webnssdb` run 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.

#### Default Mode:

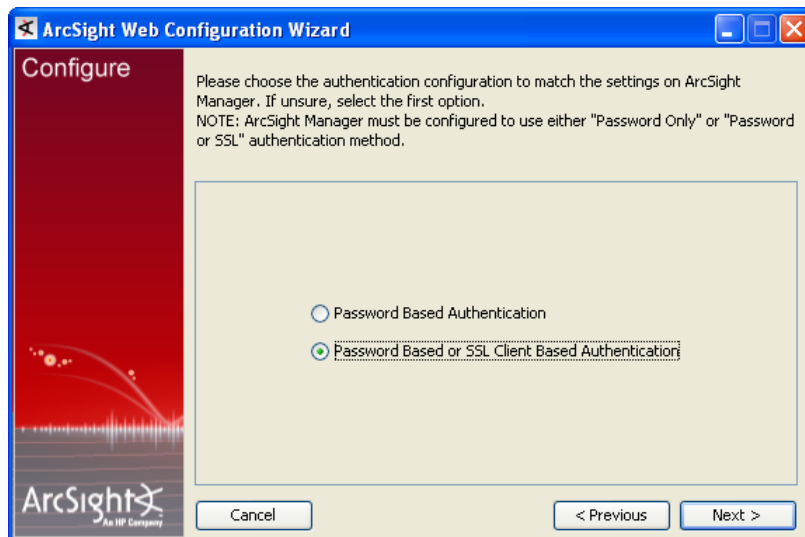
You are required to import the CAC card's root CA certificate into Web's <ARCSIGHT\_HOME>\config\jetty\webtruststore directory. For details on how to do this, see the ESM Administrator's Guide.

#### 4 Set the Authentication Option in ArcSight Web

Set ArcSight Web's authentication to **Password Based or SSL Client Based Authentication**. To do so,

- a Stop ArcSight Web.
- b Run the setup program from ArcSight Web's bin directory:
 

```
arcsight webserversetup
```
- c Select **Password Based or SSL Client Based Authentication** in the following screen.



- d Complete the setup by following the prompts in the next few screens.
- e Start ArcSight Web by entering the following from ArcSight Web's \bin directory:
 

```
arcsight webserver
```

- f Make sure to set your browser to use TLS. Follow the instructions in [“Configure Your Browser for FIPS” on page 197](#) 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, be sure to configure it to be FIPS compliant.

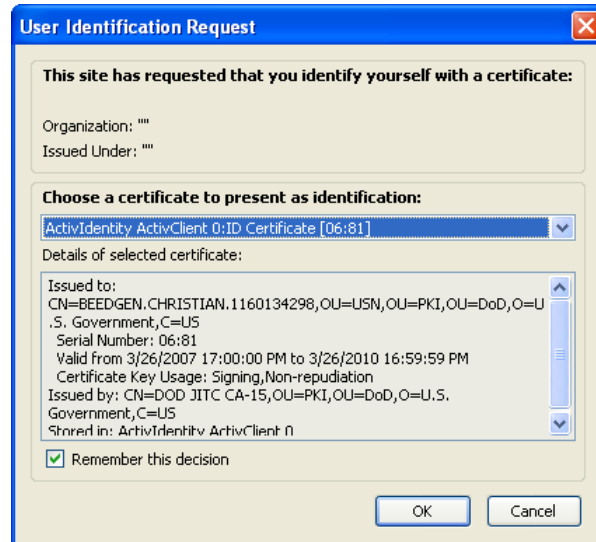
## Logging in to ArcSight Web Using CAC

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 this web site (fill in the appropriate host name): `https://<hostname>:9443/`.
- 3 You will be requested to enter your PIN



If using Firefox, you will see an exception. Click 'Add exception', then generate and confirm the certificate key. You will see the following dialog. Click **OK**.





# About ESM Locales and Encodings

---

This appendix covers the following topics:

[“Terminology” on page 229](#)

[“Before you Install a Localized Version of ArcSight ESM” on page 230](#)

[“Localization of Date Formats in Tokens and Operations” on page 233](#)

[“Key-Value Parsers for Localized Devices” on page 233](#)

[“Installing the Language Update” on page 236](#)

[“List of possible values for the agent.parser.locale.name property” on page 236](#)

ArcSight ESM is translated into various languages, for instance Japanese, traditional Chinese, simplified Chinese, French, and Korean. Setting the Locale for any of these languages ensures that you get the appropriate environment in terms of language settings, number format, date/time format, timezone settings, and Daylight Saving Time setting for that country or language. This document describes the updates to be taken into consideration when configuring ArcSight ESM for a supported language.

## Terminology

Some of the common terms used in this document are described below.

### Internationalization

Internationalization is the process of designing an application so that it can be adapted to various languages and regions without further engineering changes.

### Locale

Locale refers to the specific language of the region where you are running ArcSight ESM.

### Character Set

A character set is a collection of characters that have been grouped together for a particular purpose. An example of a character set is the English alphabet.

### Code Set

Each character in a character set is assigned a unique value. Collectively, these values are known as a code set.

## Code Point

Each character value within a code set is referred to as a code point.

## Encoding

Encoding specifies how each character's code point is stored in memory or disk files.

## Unicode

Unicode is a universal character set that assigns a unique code point to characters from all major languages of the world.

## Before you Install a Localized Version of ArcSight ESM



Keep in mind that the ArcSight Manager, Database, and Console should all be configured with the same locale.

Keep in mind that the ArcSight Manager, Database, and Console should all be configured with the same locale.

By default, all communication between ArcSight components is done using UTF-8 character encoding. Even though ArcSight ESM supports only UTF-8 internally, if your Connector receives events in UTF-16, for example, the events are still stored correctly since these events get converted to UTF-8 by the Connector before they are passed on to the Manager. The Manager then passes these events to the database where they are converted to the language-specific encoding you selected while installing the database before being persisted.



### On Windows only:

If your Operating System was installed in a particular locale, but you changed the locale later on your desktop environment to another language, the locale that was set during the OS installation will take precedence for the applications that run as a service. For instance, in such a scenario, ArcSight webserver running as a service will adopt the locale in which the operating system was installed.

To work around this, edit the service settings for the webserver and change it to run as the user who changed the locale on the desktop. This will allow you to view the ArcSight Web application in the locale that was set on your desktop environment.

To change the settings for a service,

- 1 Right click the service and select **Properties**.
  - 2 Click the **Logon** tab.
  - 3 Select **This account** and browse to the user account that had changed the locale and enter that account's password.
  - 4 Click **OK**.
-

## ArcSight Database

Before you install ArcSight Database, decide on an encoding scheme, such as UTF-8.



You cannot make changes to the encoding after you have installed the database. Any change will require reinstallation.

## Selecting an Encoding

You can choose between UTF-8 and pre-defined language-specific encodings during database installation. The advantage of using UTF-8 is that it supports all major languages in the world, so no data is lost when it is saved in the database. On the other hand, UTF-8 requires more space to store certain characters than the character's language-specific encoding. For example, if a certain Japanese character can be stored in two bytes using JA16SJIS encoding, the same character might take 3 bytes if stored in UTF-8.

Select an encoding in the following database installation screen:

**ArcSight Oracle Installation Wizard**  
Install  
Please specify instance parameters.

ORACLE\_SID: arcsight

ArcSight Database Template: ArcSight\_Large.dbt

Database Character Set: Unified\_UTF8

Allowed TNS Clients: English, French, Japanese, Chinese\_Simplified, Chinese\_Traditional, Korean, Unified\_UTF8

Cancel < Previous

| Name                | Character Set  |
|---------------------|----------------|
| English             | WE8MSWIN1252   |
| French              | WE8ISO8859P1   |
| Japanese            | JA16SJIS       |
| Chinese_Simplified  | ZHS16CGB231280 |
| Chinese_Traditional | ZHT1681G5      |
| Korean              | KO16KSC5601    |
| Unified_UTF8        | UTF8           |

The name English represents all western European languages. If you need to use a character set not shown above, consult ArcSight Installation & Configuration Guide for instructions on how to set it properly

If you anticipate that you will be storing events in multiple languages, choose a character set (encoding) that is compatible with ALL languages you intend to use. For more than one non-English language, you should choose UTF-8.

If you select UTF-8, you will be required to select the language in which you want the standard content to be installed on the database.



If you already have the database installed with an encoding other than Unified\_UTF8, but would like to change the encoding to Unified\_UTF8, you have to re-install the database and select Unified\_UTF-8 Database Character Set when prompted during the installation.

## ArcSight Manager

Install the ArcSight Manager on an Operating System that is of the same language as the language you selected while installing the database. During startup, ArcSight Manager automatically detects and uses the locale from the Operating System.

## ArcSight Console

Install the ArcSight Console on an Operating System that is of the same language as the language you selected while installing the database. During startup, ArcSight Console automatically detects and uses the locale from the Operating System.

## ArcSight SmartConnectors

If a device is configured to use a language-specific encoding (not Unicode), the Connector receiving events from this device should be configured to use the same encoding as the device.

### Setting the Encoding for Selected SmartConnectors

You can set the encoding to a character set corresponding to your Locale for the following SmartConnectors only:

- SAP Real-Time Security Audit Multi-Folder Connector.  
See the SmartConnector for SAP Real-time Security Audit Multi-Folder Configuration Guide for instructions on how to configure the encoding for this Connector.
- IBM DB2 Audit File Connector.

See the SmartConnector for IBM DB2 Audit File Configuration Guide for instructions on how to configure the encoding for this Connector.

- Oracle SYSDBA Audit Multi-Folder Connectors

See the SmartConnector for Oracle SYSDBA Audit Multi-Folder Configuration Guide for instructions on how to configure the encoding for this Connector.

The above SmartConnectors support all character sets supported by Java.



You need to change the encoding to match the log files' encoding only if the log files use an encoding other than the default one.

**Note**

Connectors not mentioned above use the default encoding of the Operating System on which they reside. Each Operating System comes with default encodings for various languages of the world. So, the encoding used in a Connector is either based on the character set that you selected when installing the ArcSight Database or the Operating System you are using.

## Localization of Date Formats in Tokens and Operations

If your Connector receives logs that contain timestamps in a non-English language or a date format that is customarily used by a non-English locale (for example, "mai 24, 2006 12:56:07.615" where "mai" is German for May) that your Connector is set to, configure the `agent.parser.locale.name` property in the `agent.properties` file. This file is located in `ARCSIGHT_HOME/current/user/agent` directory.

Set the `agent.parser.locale.name` property to the value that corresponds to the Connector's locale. By default, this property is set to `en_US`. Refer to the table at the end of this document under section "List of possible values for the `agent.parser.locale.name` property" for possible values for this property.

## Key-Value Parsers for Localized Devices

Some localized devices not only send localized Values but also localized Keys in event messages. In such a case, additional processing may be needed to translate the Keys to English for the event messages to be properly parsed. For example, assume that the content of a key-value parser is:

```
event.destinationUserName=User
```

And the received event message is:

User= 김? where 김 is Korean for KIM.

In that case, the parser as it is works fine since double byte is supported already.

If the received event message is:

우새르=김 where 우새르 is Korean for User.

Then additional mapping is needed to translate ??? to User.

If you encounter a need for a localized device, please contact Customer Support using the HP SSO website.

Windows Event Log Connector supports the following locales to parse the non-English language Keys in the Windows Event Log description:

- ja (Japanese)
- de (German)
- zh\_CN (Simplified Chinese)
- zh\_TW (Traditional Chinese)

Please call Customer Support for assistance with other non-supported languages.

## Examples

The following examples cover two different scenarios.

### Scenario 1 - Events received in a single language only

This scenario describes what you need to do when your Connector(s) receive data in a single language only, for instance Japanese. In ESM, the default encoding for Japanese is JA16SJIS.

#### Database

While installing the database, in the ArcSight Oracle Installation Wizard, select one of the following Database Character Set drop down menu:

- Japanese
- Unified\_UTF8

If you select **Japanese**, the database uses JA16SJIS encoding when saving the data into the database.

If you select **Unified\_UTF8**, you also need to select **Japanese** in the ArcSight Database Schema Initialization screen to ensure that the default system resources get installed in Japanese.

Keep in mind, some characters might take 3 bytes when stored in UTF-8 but might take only 2 bytes when stored in JA16SJIS.

#### ArcSight Manager, Console, and Web

You need to install the ArcSight Manager, Console, and Web on a Japanese Operating System. On startup, these components automatically pick up and use the locale from the Operating System.

### Scenario 2 - Events received in multiple languages

This scenario is an example of what you need to do when you are dealing with multiple Connectors that receive data in different languages.

#### Database

When you install the database, in the ArcSight Oracle Installation Wizard:

- 1 Select **Unified\_UTF8** from the Database Character Set dropdown menu. This ensures that no data is lost in translation when persisted in the database.
- 2 In the ArcSight Database Schema Initialization screen, select the language in which you want the standard content resources to be installed.

## ArcSight Manager, Console, and Web

When you installed the ArcSight Database you selected a language in which to install the system resources. You should install the ArcSight Manager, Console, and Web on an Operating System of that same language. On startup, these components automatically pick up the locale from the Operating System.

## Preparing to Install the Language Update

If you are currently running ESM v4.0 GA and would like to switch to a localized version, you need to upgrade your ESM installation (ArcSight Database, Manager, Console, and Web server) to v4.0 SP1.



While upgrading your database to v4.0 SP1, make sure that the character set you select during the upgrade is compatible with the one that you had selected when installing your existing database.

Once your system is running ESM v4.0 SP1, you need to install the language update.

## Verifying the Character Set used on your Database

If you currently use ESM v4.0 SP1, your database already has a character set specified. Follow this procedure to validate the character set that was selected when the v4.0 SP1 database was installed:

- 1 Run the following command from ARCSIGHT\_HOME/bin directory:

```
arcdbutil sql
```

- 2 When prompted for user-name, enter:

```
/ as sysdba
```

- 3 Run the following SQL statement:

```
SQL>select "PARAMETER", "VALUE" from SYS.GV_$NLS_PARAMETERS
where PARAMETER='NLS_CHARACTERSET';
```



You can only set the encoding during database installation. To change the encoding after installation, you need to reinstall ArcSight Database.

The following character sets (encodings) are supported for ArcSight Database:

| Language           | Character Set  |
|--------------------|----------------|
| English            | WE8MSWIN1252   |
| Japanese           | JA16SJIS       |
| Chinese_Simplified | ZHS16CGB231280 |

|                     |             |
|---------------------|-------------|
| Chinese_Traditional | ZHT16BIG5   |
| Korean              | KO16KSC5601 |
| Unified_UTF8        | UTF-8       |

## Installing the Language Update

By now, your database should be set to the encoding of your choice. If you have not already done so, please follow the instructions in "Verifying the Encoding used on your Database" section above to verify the database encoding, before you proceed.

You need to install the language update on ArcSight Manager, Console and Web. Refer to the Release Notes for the Language Update for installation instructions.

## List of possible values for the agent.parser.locale.name property

The table below lists the possible values for this property.

| Values | Language   | Country              | Variant |
|--------|------------|----------------------|---------|
| ar     | Arabic     |                      |         |
| ar_AE  | Arabic     | United Arab Emirates |         |
| ar_BH  | Arabic     | Bahrain              |         |
| ar_DZ  | Arabic     | Algeria              |         |
| ar_EG  | Arabic     | Egypt                |         |
| ar_IQ  | Arabic     | Iraq                 |         |
| ar_JO  | Arabic     | Jordan               |         |
| ar_KW  | Arabic     | Kuwait               |         |
| ar_LB  | Arabic     | Lebanon              |         |
| ar_LY  | Arabic     | Libya                |         |
| ar_MA  | Arabic     | Morocco              |         |
| ar_OM  | Arabic     | Oman                 |         |
| ar_QA  | Arabic     | Qatar                |         |
| ar_SA  | Arabic     | Saudi Arabia         |         |
| ar_SD  | Arabic     | Sudan                |         |
| ar_SY  | Arabic     | Syria                |         |
| ar_TN  | Arabic     | Tunisia              |         |
| ar_YE  | Arabic     | Yemen                |         |
| be     | Belarusian |                      |         |
| be_BY  | Belarusian | Belarus              |         |

| Values | Language  | Country            | Variant |
|--------|-----------|--------------------|---------|
| bg     | Bulgarian |                    |         |
| bg_BG  | Bulgarian | Bulgaria           |         |
| ca     | Catalan   |                    |         |
| ca_ES  | Catalan   | Spain              |         |
| cs     | Czech     |                    |         |
| cs_CZ  | Czech     | Czech Republic     |         |
| da     | Danish    |                    |         |
| da_DK  | Danish    | Denmark            |         |
| de     | German    |                    |         |
| de_AT  | German    | Austria            |         |
| de_CH  | German    | Switzerland        |         |
| de_DE  | German    | Germany            |         |
| de_LU  | German    | Luxembourg         |         |
| el     | Greek     |                    |         |
| el_GR  | Greek     | Greece             |         |
| en     | English   |                    |         |
| en_AU  | English   | Australia          |         |
| en_CA  | English   | Canada             |         |
| en_GB  | English   | United Kingdom     |         |
| en_IE  | English   | Ireland            |         |
| en_IN  | English   | India              |         |
| en_NZ  | English   | New Zealand        |         |
| en_US  | English   | United States      |         |
| en_ZA  | English   | South Africa       |         |
| es     | Spanish   |                    |         |
| es_AR  | Spanish   | Argentina          |         |
| es_BO  | Spanish   | Bolivia            |         |
| es_CL  | Spanish   | Chile              |         |
| es_CO  | Spanish   | Columbia           |         |
| es_CR  | Spanish   | Costa Rica         |         |
| es_DO  | Spanish   | Dominican Republic |         |
| es_EC  | Spanish   | Ecuador            |         |
| es_ES  | Spanish   | Spain              |         |
| es_GT  | Spanish   | Guatemala          |         |

| Values | Language  | Country     | Variant |
|--------|-----------|-------------|---------|
| es_HN  | Spanish   | Honduras    |         |
| es_MX  | Spanish   | Mexico      |         |
| es_NI  | Spanish   | Nicaragua   |         |
| es_PA  | Spanish   | Panama      |         |
| es_PE  | Spanish   | Peru        |         |
| es_PR  | Spanish   | Puerto Rico |         |
| es_PY  | Spanish   | Paraguay    |         |
| es_SV  | Spanish   | El Salvador |         |
| es_UY  | Spanish   | Uruguay     |         |
| es_VE  | Spanish   | Venezuela   |         |
| et     | Estonian  |             |         |
| et_EE  | Estonian  | Estonia     |         |
| fi     | Finnish   |             |         |
| fi_FI  | Finnish   | Finland     |         |
| fr     | French    |             |         |
| fr_BE  | French    | Belgium     |         |
| fr_CA  | French    | Canada      |         |
| fr_CH  | French    | Switzerland |         |
| fr_FR  | French    | France      |         |
| fr_LU  | French    | Luxembourg  |         |
| hi_IN  | Hindi     | India       |         |
| hr     | Croatian  |             |         |
| hr_HR  | Croatian  | Croatia     |         |
| hu     | Hungarian |             |         |
| hu_HU  | Hungarian | Hungary     |         |
| is     | Icelandic |             |         |
| is_IS  | Icelandic | Iceland     |         |
| it     | Italian   |             |         |
| it_CH  | Italian   | Switzerland |         |
| it_IT  | Italian   | Italy       |         |
| iw     | Hebrew    |             |         |
| iw_IL  | Hebrew    | Israel      |         |
| ja     | Japanese  |             |         |
| ja_JP  | Japanese  | Japan       |         |

| Values   | Language   | Country     | Variant |
|----------|------------|-------------|---------|
| ko       | Korean     |             |         |
| ko_KR    | Korean     | Korea       |         |
| lt       | Lithuanian |             |         |
| lt_LT    | Lithuanian | Lithuania   |         |
| lv       | Latvian    |             |         |
| lv_LV    | Latvian    | Latvia      |         |
| mk       | Macedonian |             |         |
| mk_MK    | Macedonian | Macedonia   |         |
| nl       | Dutch      |             |         |
| nl_BE    | Dutch      | Belgium     |         |
| nl_NL    | Dutch      | Netherlands |         |
| no       | Norwegian  |             |         |
| no_NO    | Norwegian  | Norway      |         |
| no_NO_NY | Norwegian  | Norway      | Nynorsk |
| pl       | Polish     |             |         |
| pl_PL    | Polish     | Poland      |         |
| pt       | Portuguese |             |         |
| pt_BR    | Portuguese | Brazil      |         |
| pt_PT    | Portuguese | Portugal    |         |
| ro       | Romanian   |             |         |
| ro_RO    | Romanian   | Romania     |         |
| ru       | Russian    |             |         |
| ru_RU    | Russian    | Russia      |         |
| sk       | Slovak     |             |         |
| sk_SK    | Slovak     | Slovakia    |         |
| sl       | Slovanian  |             |         |
| sl_SI    | Slovanian  | Slovenia    |         |
| sq       | Albanian   |             |         |
| sq_AL    | Albanian   | Albania     |         |
| sv       | Swedish    |             |         |
| sv_SE    | Swedish    | Sweden      |         |
| th       | Thai       |             |         |
| th_TH    | Thai       | Thailand    |         |
| th_TH_TH | Thai       | Thailand    | TH      |

| Values | Language   | Country   | Variant |
|--------|------------|-----------|---------|
| tr     | Turkish    |           |         |
| tr_TR  | Turkish    | Turkey    |         |
| uk     | Ukrainian  |           |         |
| uk_UA  | Ukrainian  | Ukraine   |         |
| vi     | Vietnamese |           |         |
| vi_VN  | Vietnamese | Vietnam   |         |
| zh     | Chinese    |           |         |
| zh_CN  | Chinese    | China     |         |
| zh_HK  | Chinese    | Hong Kong |         |
| zh_TW  | Chinese    | Taiwan    |         |

# Index

---

## A

- ACE/Server
  - configuring to allow RADIUS requests 155
  - establishing user accounts 156
  - installing and installing as service 155
  - migrating from internal authentication 157
- Active Directory
  - setting up authentication for 95
- Administrator account
  - Manager 101
- Administrator user 27, 78, 79, 101
- appendix
  - example of 149, 161, 167, 171, 201, 215, 229
- archive
  - volume 39
- archiving
  - uncompressed files 149
- ArcSight Console
  - client authentication 121
  - connecting to the Manager 119
  - installing 115, 116
  - reconfiguring 127
  - reconnecting to Manager 127
  - starting 125
  - uninstalling 128
  - user logs and preferences 123
  - web browser configuration 122
- ArcSight database
  - installation files 46
  - preparing your platform 42
  - reconfiguring 71
  - restarting 71
  - selecting a template 41
  - success factors for installation 33
  - uninstalling 80
- ArcSight Web 24, 82, 129
  - connecting 139
  - installing 130
  - overview 14
  - starting manually 139
  - styling 140
  - supported platforms 82, 129
  - uninstalling 140
- asset
  - defining 143
- asset categories 146
- authentication 92
  - Active Directory 95
  - external 92
  - LDAP 98
  - RADIUS 94

## C

- character set 118
- client authentication
  - ArcSight Console 121
- configuration
  - ACE/Server to allow RADIUS requests 155
  - Manager for iDefense 159
  - partition 75
  - partition management 71
  - SSL 97, 100
  - web browser in Console 122
- connecting
  - ArcSight Console to Manager 119
  - to ArcSight Web 139
  - to database 91
- Console 13
  - installing 116
  - supported platforms 115
- control files
  - Oracle 40
- creating
  - Customers 147
  - Users 147
- custom authentication scheme 100
- Customers
  - creating 147

## D

- Data Monitors
  - tuning 147
- database 13
  - connection 91
  - determining the size of 19
  - event volume 19
  - parameters 91
  - ports 24
  - protecting 24
  - restart 71
  - selecting a template 41
- database installation
  - supported platforms 33
- database upgrade
  - supported platforms 33
- DATABASE Volume 37
- defining
  - Asset Categories 146
  - Assets 143
  - Zones 143
- deleting
  - partition archiver service 79

- deployment
  - ESM 18
- deployment scenarios
  - ESM 28
  - hierarchical deployment 30
  - high availability 29
  - simple, monolithic 28
  - test environment 31
- directory structure
  - ArcSight Installation 22

## E

- ESM 11
  - built-in security 25
  - communication overview 16
  - components 11
    - Console 13
    - Database 13
  - deployment order 18
  - deployment overview 16
  - deployment scenarios 28
  - Manager 13
  - overview 11
  - planning 19
  - securing 22
  - SmartConnector 12
  - supported platforms 18
  - what is 11
- establishing
  - user accounts in ACE/Server 156
- event volume 19
- events
  - as SNMP traps 111
  - retention policy 20
- external authentication
  - guidelines 92
  - how it works 92

## F

- failover
  - ArcSight Manager 161
  - Manager architecture for high availability 161
  - monitoring processes 164
  - script to start/stop Manager 164

## G

- guidelines
  - external authentication 92
  - security 27

## H

- hardware
  - security 26
- hierarchical deployment 30
- high availability
  - scenario 29
- hot key issue 118

## I

- iDefense database
  - configuring Manager for 159

- integrating with 159
- initializing
  - resources 59
  - schema 59
  - tablespace 59
- installing
  - ACE/Server and ACE/Server as service 155
  - ArcSight Console 116
  - ArcSight Database and Oracle 45
  - ArcSight Database software 45
  - ArcSight Manager 82
  - ArcSight SmartConnectors 141
  - ArcSight Web 130
  - directory structure 22
  - Oracle 10g 48
- installing Oracle
  - general guidelines 34
- integrating
  - with iDefense database 159

## L

- LDAP
  - setting up authentication for 98

## M

- mail server 103
  - parameters 105
- Manager 13
  - asset auto creation 107
  - configuring for RADIUS authentication 156
  - determining the topology 19
  - failover 161
  - high availability 161
  - installation files 83
  - installing 82
  - Java heap memory size 87
  - ports 23
  - protecting 22
  - reconfiguring 110
  - securing properties file 110
  - select packages 102
  - setting up administrator account 101
  - setting up as service or daemon 107
  - setting up mail server 103
  - SSL certification selection 88
  - starting and stopping 108
  - supported platforms 82
  - transferring configuration 84, 118
  - uninstalling 113
  - verifying installation 110
- migrating
  - from internal authentication to ACE/Server 157
- monitoring
  - processes in high availability environment 164

## O

- operating system
  - security 27
- Oracle
  - control files 40
  - creating a new 10g instance 52
  - guidelines for installing 34

- installing 48
- storage guidelines 34
- overview
  - ESM 11
  - ESM communication 16
  - ESM deployment 16

## P

- parameters
  - database 91
- partition
  - changing configurations 77
  - configuration parameters 75
- partition archiver
  - changing password 80
  - registering with Manager 79
  - setting up 77
  - starting and stopping 79
- partition archiver service
  - deleting 79
  - reinstalling 80
- partition management
  - configuring 71
- passwords
  - character set 118
- planning
  - ESM installation 18
- preferences
  - ArcSight Console 123
- protecting
  - ArcSight Database 24

## R

- RADIUS authentication
  - configuring Manager for 156
  - defining shorter internal login names 153
  - passcodes 153
  - set up 94
  - setting up 153
  - setting up ACE/Server 155
  - two-factor challenge responses 154
- reconfiguring
  - ArcSight Console 127
  - ArcSight Database 71
- reconnecting
  - Console to Manager 127
- recyclebin parameter 128
- REDO Volume 39
- resources
  - establishing 143
  - initializing 59
- restarting
  - ArcSight Database 71
- retention policy 20
- rules
  - tuning 147
- running
  - Manager as a Windows service 109

## S

- schema
  - initializing 59

- security 25
  - guidelines and policies 27
  - hardware 26
  - operating system 27
- setting
  - ACE/Server RADIUS authentication 155
  - RADIUS authentication 153
- shortcut key issue 118
- size
  - database 19
  - Java Heap Memory 87
  - topology of Managers 19
- SmartConnectors 12, 141
  - deployment considerations 141
  - installing 141
- SNMP field types
  - mapping to ArcSight field types 113
- SNMP traps
  - configure 111
- SSL
  - configuring 97, 100
- SSL certificate
  - selecting 88
- starting
  - ArcSight Console 125
  - ArcSight Manager 108
  - ArcSight Web manually 139
  - partition archiver 79
- stopping
  - ArcSight Manager 108
  - manually started Manager 109
  - partition archiver 79
- supported platforms
  - ArcSight Web 82, 129
  - Console 115
  - database installation and upgrade 33
  - ESM 18
  - Manager 82, 129
- SYSTEM Volume 36

## T

- tablespace
  - initializing 59
- test environment
  - example 31
- topology
  - Managers 19
- troubleshooting
  - communication between ACE/Server and Manager 157
- tuning
  - data monitors 147
  - rules 147

## U

- UNCOMPRESSED Archive types 149
- uncompressed files
  - archiving 149
  - examples of archiving 149
- uninstalling
  - ArcSight Console 128
  - ArcSight Database 80
  - ArcSight Web 140

upgrading  
    ArcSight Database and Oracle 45  
user logs  
    ArcSight Console 123  
users  
    creating 147

## V

volume  
    ARCHIVE 39  
    DATABASE 37  
    REDO 39

SYSTEM 36

## W

Web 14  
Web browser  
    configuring in Console 122

## Z

zones  
    defining 143