

Upgrading ArcSight™ ESM

v4.0 SP3 to v4.5 SP1

April 20, 2009



Upgrading ArcSight™ ESM v4.0 SP3 to v4.5 SP1

Copyright © 2009 ArcSight, Inc. All rights reserved.

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

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

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
04/20/09	Upgrading ArcSight ESM	v4.0 SP3 to v4.5 SP1

Document template version: 1.0.2.7

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://forum.arcsight.com

Contents

Chapter 1: Preparing for Upgrade	1
Document Status	1
Summary	1
Downloading installation files, scripts, and other documents	2
Chapter 2: Upgrading ArcSight Database	5
Preparing the ArcSight Database	5
Upgrading the ArcSight Database Software, Oracle, and Partition Archiver	6
Transferring Partition Archiver Settings	10
Upgrading Oracle 10.2.0.2 Instance to Oracle 10.2.0.4	12
Chapter 3: Upgrading ArcSight Manager	17
Preparing the ArcSight Manager	17
Upgrading the ArcSight Manager	18
Updating and Starting the Partition Archiver Service	28
Chapter 4: Upgrading ArcSight Consoles	29
Upgrading ArcSight Consoles	29
Chapter 5: Upgrading ArcSight Web	33
Upgrading ArcSight Web	33
Chapter 6: Upgrading ArcSight SmartConnectors	37
Chapter 7: Checking the State of Existing Content After Upgrade	39
Index	41

Chapter 1

Preparing for Upgrade

Document Status

The information in this note applies to ArcSight ESM v4.0 SP3 or later.

Summary

This technical note describes the steps required to upgrade the ArcSight ESM from v4.0 SP3 to v4.5 SP1.



Starting with ESM v4.0 SP2, ArcSight ESM supports the Federal Information Processing Standard 140-2 (**FIPS** 140-2), as an alternative to running ESM in **default mode** (non-FIPS). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive but Unclassified (SBU) information should meet these standards. You need not upgrade your ESM to FIPS 140-2 mode if you are not required to do so.



Make sure that you also read the "How Standard Content is Installed and Upgraded" section in the System Content Reference Guide before you proceed with the upgrade to understand how the installer upgrades existing ArcSight supplied content and customer-created content. You can download the System Content Reference Guide from ArcSight Customer Support download site.

If you have a hierarchical or a multi-Manager ESM setup, also see the technical note *Upgrading Hierarchical or Other Multi-Manager ArcSight™ ESM Deployments*, available at the ArcSight Customer Support download site.

Upgrading ArcSight ESM involves the following steps:



ESM v4.5 SP1 does not support Oracle 10.2.0.2. If you are currently using Oracle 10.2.0.2, ArcSight recommends that you upgrade to Oracle 10.2.0.4 **before** you upgrade the ESM components. You will not be able to start ArcSight Manager if you have not upgraded to Oracle 10.2.0.4.

[Downloading installation files, scripts, and other documents](#)

[Upgrading ArcSight SmartConnectors](#)

[Upgrading the ArcSight Database Software, Oracle, and Partition Archiver](#)

[Upgrading ArcSight Manager](#)

[Upgrading ArcSight Consoles](#)

[Upgrading ArcSight Web](#)

[Checking the State of Existing Content After Upgrade](#)

Downloading installation files, scripts, and other documents

This section lists all the installation files, scripts, and supporting documentation that you will need during the upgrade. Unless noted, all files are available at the ArcSight Software web site (<https://software.arcsight.com>).

You can do one of the following:

- Download all files to a machine on your local network and then transfer the files to the ArcSight component machines (Manager, database, Web and Console) as needed.
- Download files directly to the component machines where they will be installed.

For the SmartConnectors:

- 1 Download installation files as appropriate for your SmartConnector platforms:

- ◆ `ArcSight-4.7.1.xxxx.0-Connector-Win.exe`
- ◆ `ArcSight-4.7.1.xxxx.0-Connector-AIX.bin`
- ◆ `ArcSight-4.7.1.xxxx.0-Connector-MacOSX.zip`
- ◆ `ArcSight-4.7.1.xxxx.0-Connector-Linux.bin`
- ◆ `ArcSight-4.7.1.xxxx.0-Connector-Solaris.bin`
- ◆ `ArcSight-4.7.1.xxxx.0-Connectors.aup` (for remote upgrade)

For the Database:

- 1 Check the current ArcSight database version you are running on the database machine. To check the version, in a v4.0 SP3 Console, click **Help | About**. The current version is displayed in 4.0.3.XXXX.n format, where XXXX is the build number and n is the patch number.
- 2 Download the database installation file appropriate for your platform. The following installation files are available:
 - ◆ `ArcSight-4.5.1.xxxx.0-DB-Win.exe`
 - ◆ `ArcSight-4.5.1.xxxx.0-DB-AIX.bin`
 - ◆ `ArcSight-4.5.1.xxxx.0-DB-Linux.bin`
 - ◆ `ArcSight-4.5.1.xxxx.0-DB-Solaris.bin`
- 3 If you need to upgrade your Oracle 10.2.0.2 installation to Oracle 10.2.0.4, download the Oracle 10.2.0.4 files appropriate for your platform. Do not extract the contents of the files you copy.

These files are available for Oracle 10.2.0.4.

Platform	Oracle 10g Database Files
64-bit	32-bit

Platform	Oracle 10g Database Files	
Windows	x86-64 (AMD64): 102010_win64_x64_database.zip p6810189_10204_MSWIN-x86-64.zip	IA32: 10201_database_win32.zip p6810189_10204_win32.zip
Linux	x86-64 (AMD64): 10201_database_linux_x86_64.cpio.gz p6810189_10204_Linux-x86-64.zip	IA32: 10201_database_linux32.zip p6810189_10204_Linux-x86.zip
AIX	10gr2_aix5l64_database.cpio.gz p6810189_10204_AIX5L.zip	
Solaris	10gr2_db_sol.cpio.gz p6810189_10204_solaris-64.zip	

You should download the Oracle OPatch and CPU files and apply the CPU. See the Release Notes for the product for details on installing the CPU.

For the Manager:

- 1 Check the current ArcSight ESM version you are running on the Manager. To check the version, in a v4.0 SP3 Console that connects to the Manager, click **Help** | **About**. The current version is displayed in 4.0.3.XXXX.n format, where XXXX is the build number and n is the patch number.

- 2 Download the Manager installation file, as appropriate for your platform. These installation files are available:

- ◆ ArcSight-4.5.1.xxxx.0-Manager-Win.exe
- ◆ ArcSight-4.5.1.xxxx.0-Manager-Win64.exe
- ◆ ArcSight-4.5.1.xxxx.0-Manager-AIX.bin
- ◆ ArcSight-4.5.1.xxxx.0-Manager-Linux.bin
- ◆ ArcSight-4.5.1.xxxx.0-Manager-Linux64.bin
- ◆ ArcSight-4.5.1.xxxx.0-Manager-Solaris.bin

For the Consoles:

Download the Console installation file, as appropriate for your platform. The following installation files are available:

- ◆ ArcSight-4.5.1.xxxx.0-Console-Win.exe
- ◆ ArcSight-4.5.1.xxxx.0-Console-Linux.bin
- ◆ ArcSight-4.5.1.xxxx.0-Console-MacOSX.bin
- ◆ ArcSight-4.5.1.xxxx.0-Console-Solaris.bin

For ArcSight Web:

Download the ArcSight Web installation file, as appropriate for your platform. The following installation files are available:

- ◆ ArcSight-4.5.1.xxxx.0-Web-Win.exe
- ◆ ArcSight-4.5.1.xxxx.0-Web-AIX.bin
- ◆ ArcSight-4.5.1.xxxx.0-Web-Linux.bin
- ◆ ArcSight-4.5.1.xxxx.0-Web-Solaris.bin

Other Documentation:

In addition to this technical note, you may need to refer to the following documents to complete the upgrade process:

- ArcSight ESM Installation and Configuration Guide, v4.5 SP1
- ArcSight ESM Administrator's Guide, v4.5 SP1
- ArcSight ESM System Content Reference Guide
- Upgrading Hierarchical or Other Multi-Manager ArcSight™ ESM Deployments

These documents are available on the ArcSight Customer Support download site.



Make sure that you have the Firefox web browser installed and available in PATH before you begin the upgrade. The installer uses Firefox to display the upgrade context report after the upgrade is done. If you do not setup Firefox, you will see a `java.io.IOException: firefox: not found` exception at the end of `managerwizard.log`. You will have to manually open the upgrade summary report from `"<path_of_manager>/upgrade/out/<timestamp>/summary.html"` using any available browser on your system.

Upgrading ArcSight Database

Preparing the ArcSight Database

Before you proceed with the upgrade, prepare your ArcSight database as follows:

- 1 The following table lists the database machines and versions supported for v4.5 SP1. Verify that your database machine and version is supported.

Operating System	Database	Typical System Configuration
Windows Server 2003 R2 SP2 (32-bit and 64-bit)	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Red Hat Enterprise Linux 4.0 AS (RHEL 4 AS), update 7 (32-bit and 64-bit) Red Hat Enterprise Linux 5.0 AS (RHEL 5.3 AS), update 2 (32-bit and 64-bit) SUSE Linux 10 SP2 Enterprise Server (64-bit)	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Sun Solaris 10 (64-bit)	Oracle 10.2.0.4	Sparc-compatible multi-CPU system with 2-16 GB RAM
IBM AIX 5L, Version 5.3 (5.3.0.70) (64-bit)	Oracle 10.2.0.4	Power PC multi-CPU system with 2-16 GB RAM, 2 GB disk space

See About Applying an Oracle Patch or Patch Set in ArcSight ESM Installation and Configuration Guide, v4.5 SP1 for additional steps you must perform if you apply an Oracle patch or patch set to this configuration.



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

- 2 If you are upgrading your Oracle 10.2.0.2 installation, you can use ArcSight Database v4.5 SP1 installer as described in this document to upgrade to Oracle 10.2.0.4.
- 3 If you downloaded the latest patch for your ArcSight database, install it.

Instructions to install the patch are available in Release Notes that you downloaded with the patch.

4 Perform these steps to identify if your v4.0 SP3 database is ready for upgrade:

a (Optional) Shut down your v4.0 SP3 ArcSight Manager.

The `dbcheck` script provides more accurate time estimates for index upgrade if it is run when ArcSight Manager is shut down.

For instructions about shutting down your ArcSight Manager, see *ArcSight ESM Administrator's Guide, v4.0 SP3*.

b In `ARCSIGHT_HOME/bin` of your v4.0 SP3 database installation, run the following command:

```
arcsight dbcheck
```

The command generates the following four log files in the `logs/dbcheck` directory. In addition, the command packs the generated log files in `ARCSIGHT_HOME/dbchecklogs.tar.gz` on UNIX and `ARCSIGHT_HOME/dbchecklogs.zip` on Windows..

- `DatabaseInfo.htm`—Provides basic database information
- `TablespaceInfo.htm`—Provides information such as free space, names of tablespaces, and so on
- `PartitionInfo.htm`—Provides information about partitions
- `EventIndexInfo.htm`—Provides estimates for event index upgrade

To view a log file, open the `index.html` file, located in the `logs/dbcheck` directory and click the appropriate link.

If the log files contain errors or warnings, try to resolve issues that might be causing those errors. ArcSight strongly recommends resolving all issues before proceeding with the upgrade. If you need assistance, upload the `dbchecklogs.tar.gz` or `dbchecklogs.zip` file (as appropriate for your platform) to the ArcSight Software web site and contact ArcSight Customer Support.

For instructions about starting your ArcSight Manager (if you had stopped it), see *ArcSight ESM Administrator's Guide, v4.0 SP3*.

Upgrading the ArcSight Database Software, Oracle, and Partition Archiver



Even if you choose to use your preexisting Oracle 10.2.0.4 installation, you must upgrade your ArcSight database software to v4.5 SP1.

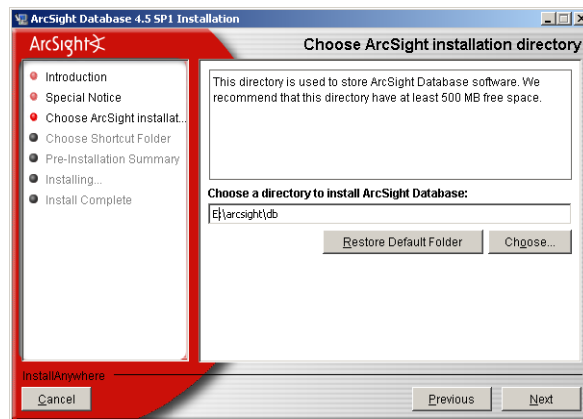


ESM v4.5 SP1 does not support Oracle 10.2.0.2. If you are currently using Oracle 10.2.0.2, ArcSight recommends that you upgrade to Oracle 10.2.0.4 **before** you upgrade the Manager. You will not be able to start ArcSight Manager if you have not upgraded to Oracle 10.2.0.4.



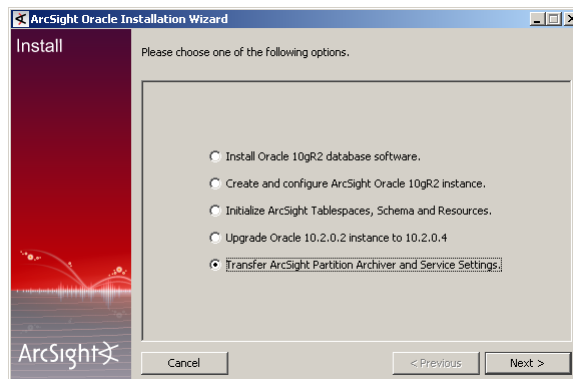
Your ArcSight Manager can be up and running until you are instructed to shut it down during the Database upgrade procedure.

- 1 Make sure to close any open connections to Oracle database before proceeding further.
- 2 If you downloaded the v4.5 SP1 Database installation file on a different machine, transfer it to your Database machine.
- 3 If you have Partition Archiver service running on your v4.0 SP3 database machine, shut it down.
- 4 Log in as "root" on the database server.
- 5 Run the database installation program.
- 6 Click **Next** in the Introduction and Special Notice screens.
- 7 Enter the location where you want to install the v4.5 SP1 database software. This location should be different from where you have the v4.0 SP3 database software installed.

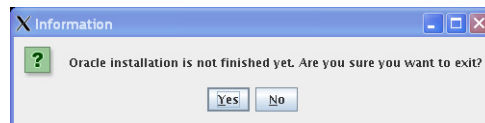


- 8 Click **Next**.
- 9 Step through the following screens:
 - ◆ **Choose Link Folder**—Specify or select where the ArcSight Database icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.
 - ◆ **Pre-Installation Summary**

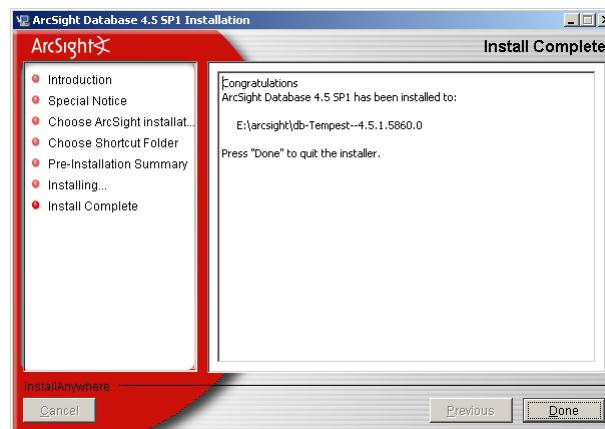
- 10** Use the bulleted points below to select an option in the following screen to suit your needs.



- ◆ If you did not have Partition Archiver configured in v4.0 SP3, Click **Cancel** and click **Yes** in the following message box:



Click **Done** in the following wizard screen and you will have finished upgrading the ArcSight Database software.



- ◆ If you have Partition Archiver configured in v4.0 SP3, you will need to transfer the Partition Archiver settings to your v4.5 SP1 ArcSight Database in addition to upgrading it. So, select **Transfer ArcSight Partition Archiver and Service Settings** and click **Next**. See ["Transferring Partition Archiver Settings" on page 10](#) for details on the wizard screens that follow.

- ◆ If you would like to upgrade your Oracle installation, select **Upgrade Oracle 10.2.0.2 instance to 10.2.0.4** and follow the instructions in the section, ["Upgrading Oracle 10.2.0.2 Instance to Oracle 10.2.0.4" on page 12.](#)



Notes about database upgrade

- The Partition Archiver service does not start automatically. Therefore, you must start the service manually once you have upgraded your Manager to v4.5 SP1. See the section, ["Updating and Starting the Partition Archiver Service" on page 28](#) in the [Upgrading ArcSight Manager](#) chapter.
- Index upgrade is not required when you upgrade from v4.0 SP3 to v4.5 SP1.

When Oracle Optimizer decides on a query execution plan, it can dynamically do a sampling of actual data to estimate the cost of the query. This will help improve query performance. To enable dynamic sampling, run the following commands:

```
% arcdbutil sql

Enter user-name: / as sysdba

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

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.



Running the [SetDynamicSampling.sql](#) is not required if you had already upgraded your database to 10.2.0.4 with 4.0 SP3 release.

```
% arcdbutil sql

Enter user-name: / as sysdba

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

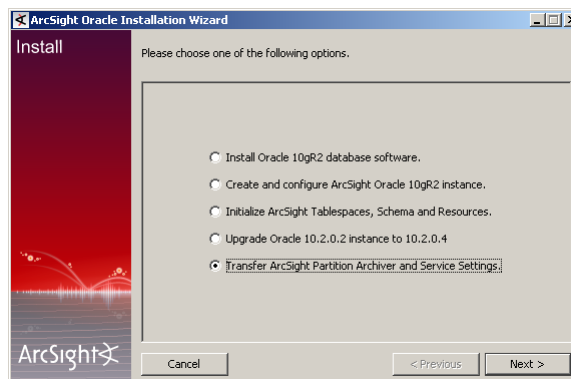


This script should be run every time you make any storage hardware changes that affects IO transfer speeds.

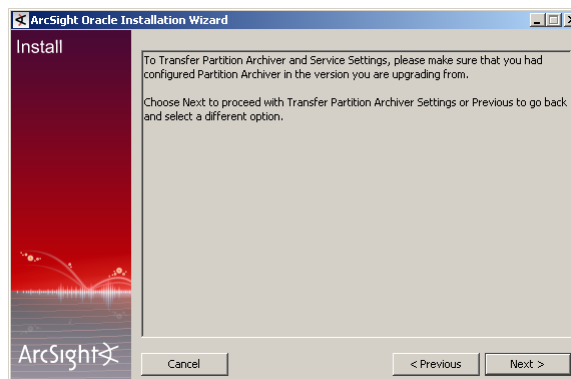
You have installed the ArcSight database v4.5 SP1 software. Go to the next section [Upgrading ArcSight Manager](#).

Transferring Partition Archiver Settings

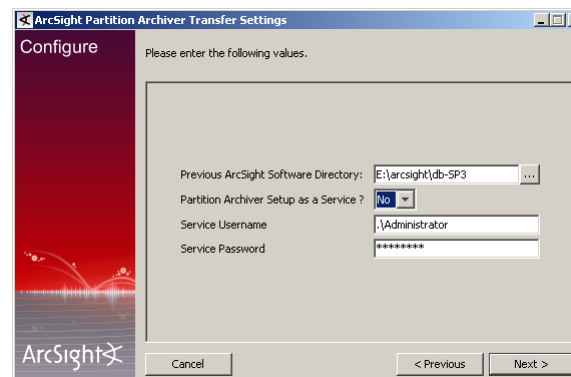
- 1 Select the **Transfer ArcSight Partition Archiver and Service Settings** option as shown:



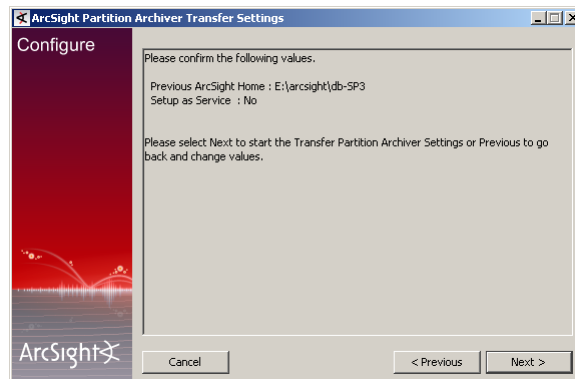
- 2 Click **Next** to confirm that you had configured the Partition Archiver in v4.0 SP3:



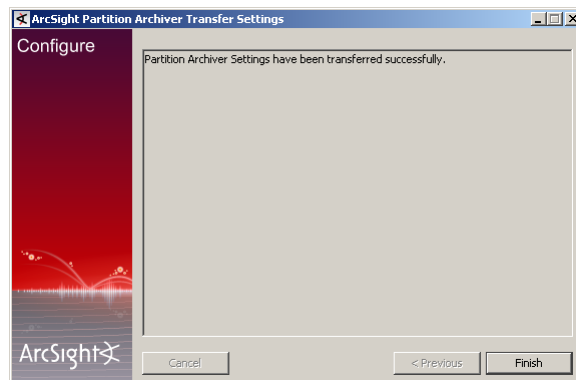
- 3 Enter the path name of the existing ArcSight Database <ARCSIGHT_HOME> in the following screen and click **Next**:



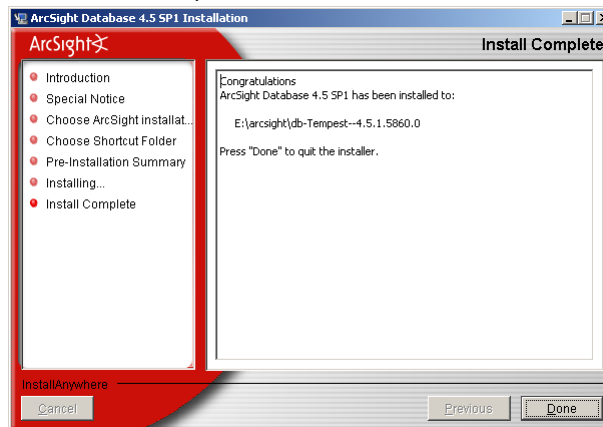
- 4 Click **Next** if you are satisfied with the settings that you have selected:



- 5 Once the Partition Archiver settings have been transferred successfully, you will see a message saying so. Click **Finish** in the screen shown below:



- 6 Click **Done** to quit the installer:



You have transferred Partition Archiver settings from your v4.0 SP3 Database installation.

Make sure to read the [“Notes about database upgrade”](#) on page 9 and follow the instructions to enable dynamic sampling following it.

Upgrading Oracle 10.2.0.2 Instance to Oracle 10.2.0.4

ESM v4.5 SP1 does not support Oracle 10.2.0.2. If your current installation uses Oracle 10.2.0.2 you are required to upgrade it to Oracle 10.2.0.4.



We suggest that you do a full backup of your database before you begin the upgrade process.

You can take a cold backup by shutting down the database and backing up the `ORACLE_HOME` and your data files directories. Make sure to restart the database after taking the backup.



Notes:

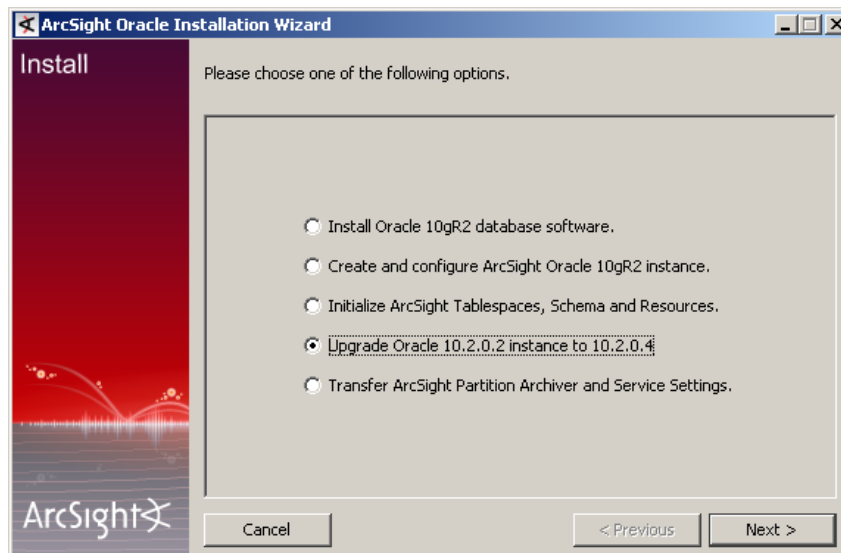
- Make sure to close any open SQL connections to Oracle database before proceeding further.
- Make sure that the TNS listener and the Oracle instance are up and running. Shut down all services.
- Make sure that the ArcSight Manager, Web, and Partition Archiver are shut down.

- 1 If you do not already have the installation/upgrade wizard running, start it by running the following from ArcSight Database's `bin` directory:

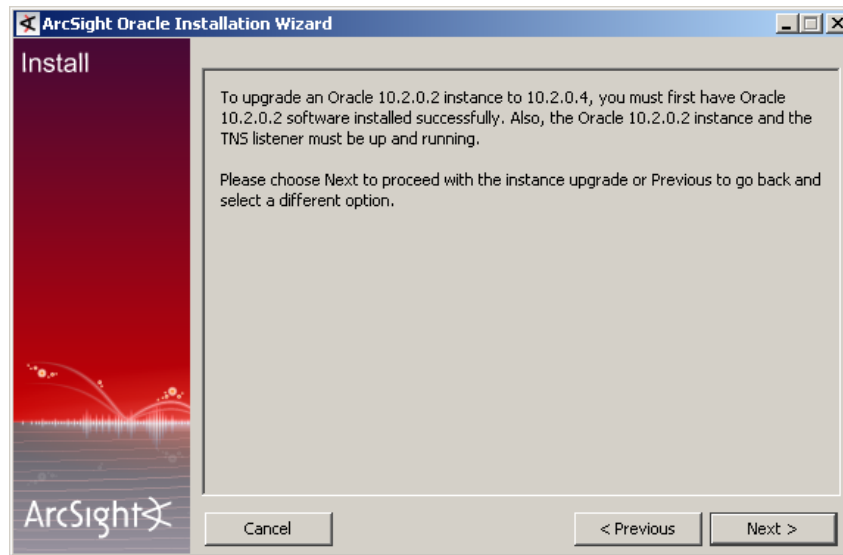
```
arcsight databasesetup
```

If you have the wizard already running, go to step 2.

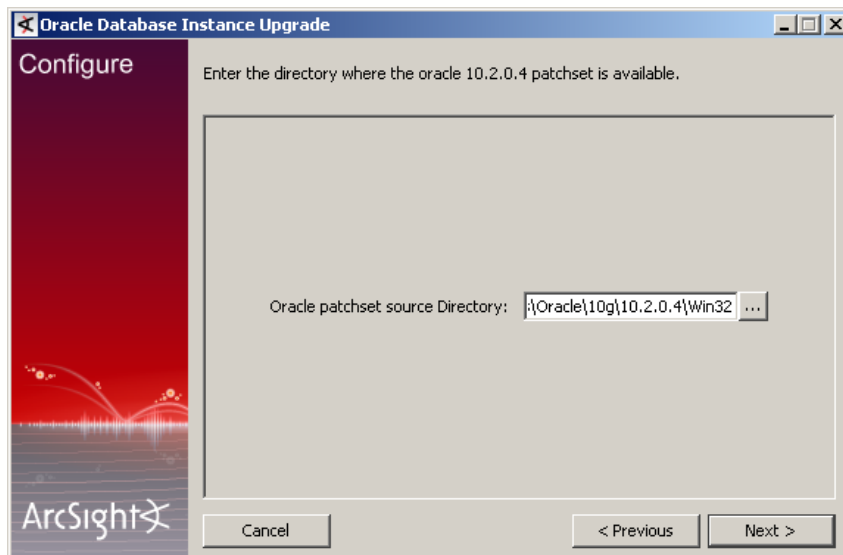
- 2 To upgrade Oracle 10.2.0.2 instance to 10.2.0.4, select the following option:



- 3 You will be prompted to make sure that you have the Oracle software installed. Click **Next**.



- 4 Enter or navigate to the location of the Oracle 10.2.0.4 source directory and click **Next**.



- 5 Enter or navigate to the location where your current v4.0 SP3 ArcSight Database exists and click **Next**.

The installation wizard uses this information to retrieve the database settings.

- 6 Enter the Oracle Admin User Password for your Oracle 10.2.0.2 installation and click **Next**.



Occasionally, the wizard does not display the ORACLE_HOME value. In that case, please enter the path to your Oracle 10.2.0.2 installation in the ORACLE_HOME textbox.

- 7 You have the option to install the Oracle Enterprise Manager.



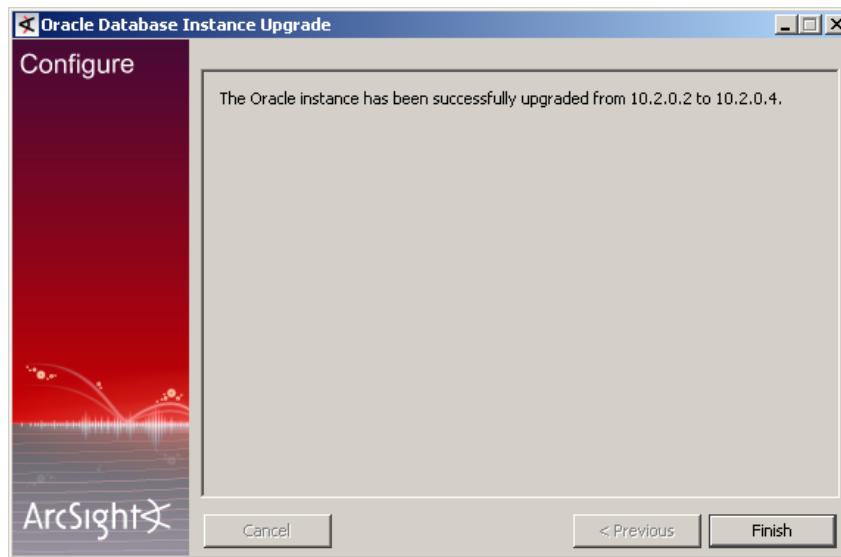
The license for Oracle Enterprise Manager is not included as a part of ArcSight's embedded Oracle license. You should only install the Oracle Enterprise Manager if you have obtained a license directly from Oracle for it.

Select **Yes** in the Configure EM? field and enter the information about the Oracle Enterprise Manager if you want to install it. If you choose not to install the Enterprise Manager, you can leave the fields blank and ignore this screen by clicking **Next**:

- 8 You will get the following screen informing you that Oracle is ready to be upgraded. Click **Next** if you do not want to make any changes to the previous panels.

- 9 While Oracle is getting upgraded, you can check the progress and status of your upgrade in the `\ORACLE_HOME\cfgtoollogs\dbca\silent.log` file.

- 10** Once the upgrade completes successfully, you will see a panel saying so.



You have finished upgrading to Oracle 10.2.0.4.

Chapter 3

Upgrading ArcSight Manager

Preparing the ArcSight Manager

The ArcSight Manager upgrade process includes upgrading the Manager software and all of ArcSight provided standard content.

Prepare ArcSight Manager as follows:

- 1 Verify that your database machine and version is supported for v4.5 SP1 from the list of supported platforms and database versions in ["Preparing the ArcSight Database" on page 5](#).
- 2 Verify that your Manager machine is supported for v4.5 SP1 from the list of supported platforms in the following table.



Make sure that you use a 64-bit installer when upgrading the Manager on a 64-bit platform.

Platform	Supported Operating System	Typical System Requirements
Linux	RHEL v4.0 AS update 7 (32 bit and 64-bit) RHEL v5.3 AS update 2 (32 bit and 64-bit) SUSE Linux 10 SP2 Enterprise Server (64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Microsoft Windows	Microsoft Windows Server 2003 R2 SP2 (32-bit and 64-bit) Microsoft Windows Server 2008 (32-bit and 64-bit)	x86-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
Solaris	Sun Solaris 10 (64-bit)	Sparc-compatible multi-CPU system with 2-4 GB RAM, 2 GB disk space.
IBM AIX	AIX 5L 5.3 (5.3.0.70) 64-bit	Power PC multi-CPU system with 2-16 GB RAM, 2 GB disk space



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

- 3 If you downloaded the latest patch for your ArcSight Manager, install it.
- 4 It is a good idea to note down the details of your customized zones, such as the start and end addresses, their location in the directory hierarchy, and so on just in case you need to restore the customization upon upgrade.
- 5 Make sure that you have run the `dbcheck` script on your database as described in “Preparing the ArcSight Database” on page 5. After running `dbcheck`, make sure that all log files the script generates are error and warning free.
- 6 Take a backup of all system resources and database definitions in your database. If the Manager upgrade process fails, you will need to restore your database to its original state before you can restart upgrade. This back up will be necessary in such a circumstance. Additionally, if you made changes to existing ArcSight-supplied resources, they will be overwritten during the upgrade. To restore your changes after the upgrade, you can use the backup copy as a reference.

To take a backup, export the database system tables as follows:

- a Log in to the ArcSight Database system as the user who installed the ArcSight Database software ('root' on UNIX and 'Administrator' on Windows, by default).
- b If your ArcSight Database was not set up using the ArcSight Database Installer, make sure that the following environment variables are set up correctly:

ORACLE_HOME—Should be set to the directory where Oracle is installed on your system

ORACLE_SID—Should be set to the ID for ArcSight Database, typically, 'arcsight'.

PATH—Should be set to `$<ORACLE_HOME>/bin:$<PATH>` on UNIX and `%<ORACLE_HOME>%\bin;%<PATH>%` on Windows.

- c In `ARCSIGHT_HOME/bin` of your v4.0 SP3 database installation, run this command:

```
arcsight export_system_tables <username>/<password>@<TNSname>
```

where <username> is the ArcSight account name on the database.

<password> is the password for the ArcSight account name.

<TNSname> is the name of the database, as specified in `tnsnames.ora`, from which to export the system tables.

Upon successful completion, the command generates two files: a temporary parameter file and the actual database dump file called `arcsight.dmp`, which contains a dump image of the system tables. This file gets created in `<ARCSIGHT_HOME>`.



Make sure to use the absolute path to the file when importing this file. You will receive an error message if you use a relative path.

Upgrading the ArcSight Manager



Do not upgrade ArcSight Manager until you have successfully upgraded ArcSight Database and successfully exported system tables as described in “Preparing the ArcSight Manager” on page 17.

Perform these steps to upgrade your Manager:

- 1 If you downloaded the v4.5 SP1 Manager installation file to a different machine, transfer it to your Manager system.

- 2 Make sure that the Manager is stopped.

For instructions about shutting down your ArcSight Manager, see *ArcSight ESM Administrator's Guide, v4.0 SP3*.

- 3 Log in as user "arcsight" on the Manager machine.

This step is required because the v4.5 SP1 Manager cannot be installed using the "root" user account for security reasons.

- 4 Run the installation command, as appropriate for your platform, from the directory where you downloaded the installation file.

For example, run `./ArcSight-4.5.1.XXXX.0-Manager-Linux.bin` on a Linux machine or on Windows, double-click on the `ArcSight-4.5.1.XXXX.0-Manager-Win.exe` file.

- 5 Step through the Installation wizard screens. Specifically, enter values as described below for the following wizard screens:

- ◆ **Choose ArcSight Installation Directory**—Enter an `<ARCSIGHT_HOME>` path for v4.5 SP1 that is different from where the existing Manager is installed.



Do NOT install v4.5 SP1 Manager in the same location as the existing Manager.

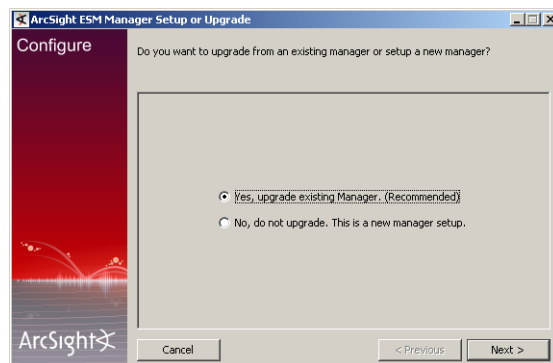
Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder (on Windows)/Choose Link Folder (on UNIX)**—Specify or select where the ArcSight Manager icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.

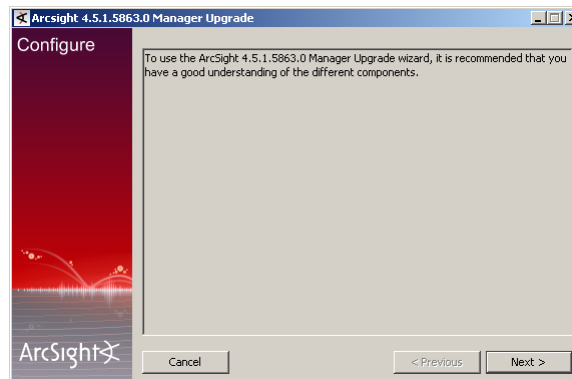
- ◆ **Pre-Installation Summary**—Review the settings and click **Next**.

After you have stepped through the Installation Wizard, it automatically starts the Configuration Wizard.

- 6 Select **Yes, upgrade existing Manager**, and Click **Next** in the following screen:

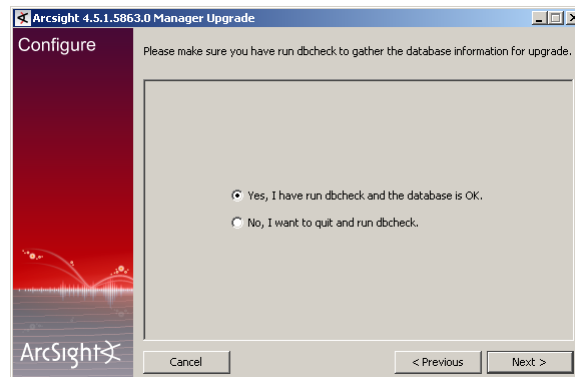


- 7 You will see the following message. Click **Next**:



- 8 If you did not run the `dbcheck` script on your database as described in “Preparing the ArcSight Database” on page 5, you must run it and make sure that all log files the script generates are error and warning free.

- ◆ To stop the Manager upgrade at this point, select **No, I want to quit and run dbcheck** and click **Next** in the following screen.

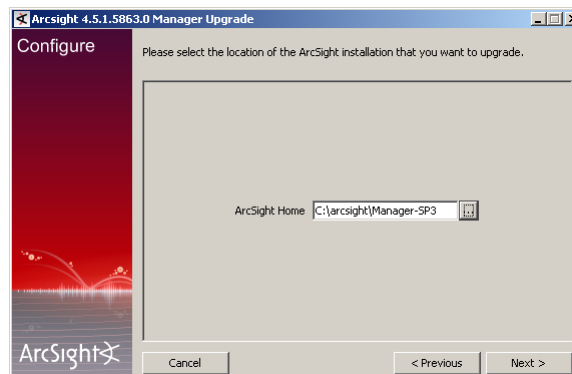


After you have run the `dbcheck` script, you can resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:

```
arcsight upgrade manager
```

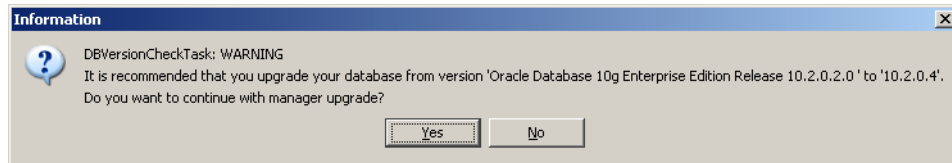
The upgrade process resumes from this point.

- ◆ To continue with Manager upgrade, select **Yes, I have run dbcheck and the database is OK** and click **Next** in the above screen.
- 9 Select the location of v4.0 SP3 installation in the following screen and click **Next**:

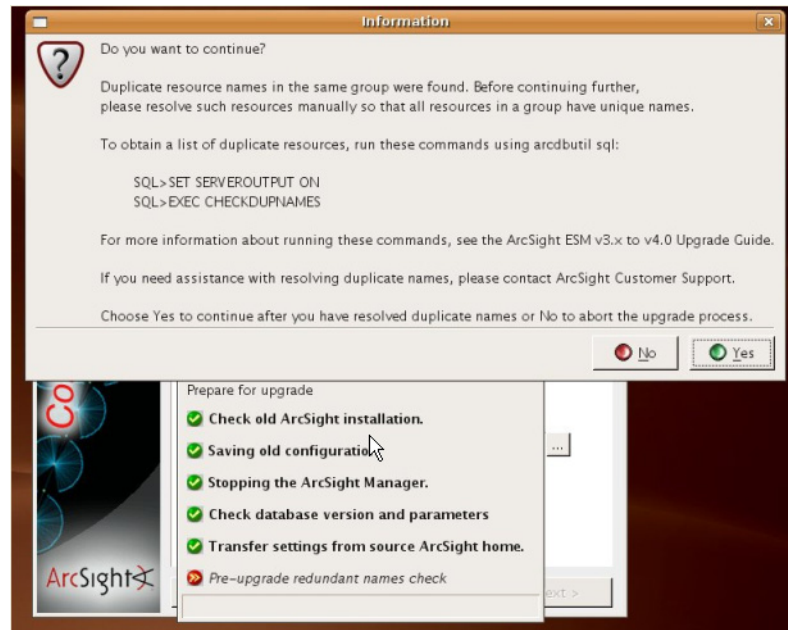


- 10** If you are using Oracle 10.2.0.2 and have not yet upgraded to Oracle 10.2.0.4, you will see a warning message telling you to upgrade your Oracle installation to 10.2.0.4.

You have the option to upgrade Oracle to 10.2.0.4 first and then continue with the Manager setup, or you can click **Yes** and continue with the Manager setup at this time and upgrade Oracle later. However, keep in mind that since Oracle 10.2.0.2 is not supported, you will be required to upgrade Oracle to 10.2.0.4 **before** you start the Manager.



- 11** A Pre-upgrade redundant name check is automatically done at this point to ensure there are no duplicate resource names in the same group in your database. If duplicate names are found, the following warning is generated:



ArcSight strongly recommends that you resolve all duplicate names before proceeding further with the upgrade.

Resolve duplicate names manually. Please contact ArcSight Customer Support if you need assistance doing this.

After you have resolved all duplicate names, click **Yes** in the above warning message to continue with the upgrade.

If for any reason, this step fails do the following:

- a** Check for duplicate resource names. Enter these commands in `ARC_SIGHT_HOME/utilities/database/oracle/common/sql` on your **database** machine to obtain a complete list of duplicate resource names:

```
../../../../../../../../bin/arcdbutil sql username/password@tnsname
```

```
SQL> SET SERVEROUTPUT ON
```

```
SQL> @CheckDupNames.sql
```

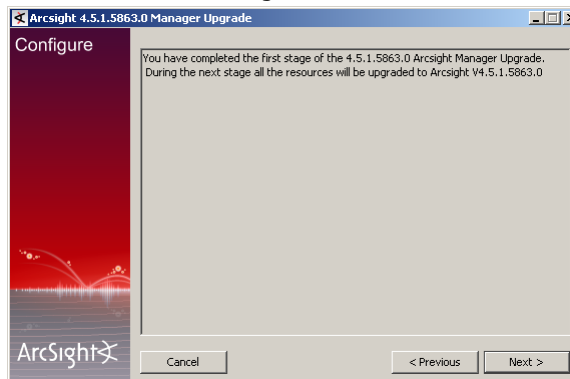
This creates the `CheckDupNames.sql` procedure.

```
SQL> EXEC CHECKDUPNAMES
```

b Resolve the duplicate names manually.

For assistance with resolving duplicate resource names, contact ArcSight Customer Support.

12 You will see the following screen:



If the Manager upgrade fails from this point forward, you must first import the v4.0 SP3 system tables you exported in ["Preparing the ArcSight Manager" on page 17](#) and then resume upgrade from [Step 4 on page 19](#).

To import system tables, run this command from your ArcSight Database's `ARCSIGHT_HOME/bin` directory:

```
arcsight import_system_tables <export_username> <import_username>  
<import_password> <TNS_name> <dump_file_path>
```

13 ArcSight's stock content is installed as follows:



For an in-depth understanding of how resources installed with ArcSight ESM have been updated, rearranged, or deprecated, see the *System Content Reference Guide*. You can download the *System Content Reference Guide* from the ArcSight Customer Support download site.

◆ Foundation content

The Foundation content is automatically installed as a part of ArcSight ESM to provide out-of-box resources that you can start using immediately to monitor and protect your network.

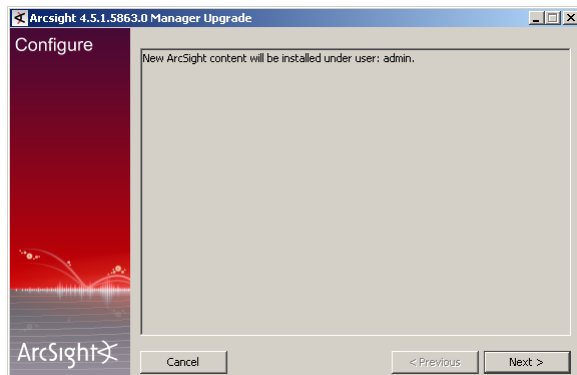
◆ System Core content

The System Core content provides the foundation building blocks for ArcSight ESM to work. This content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in `/All Filters/ArcSight System/Core`.

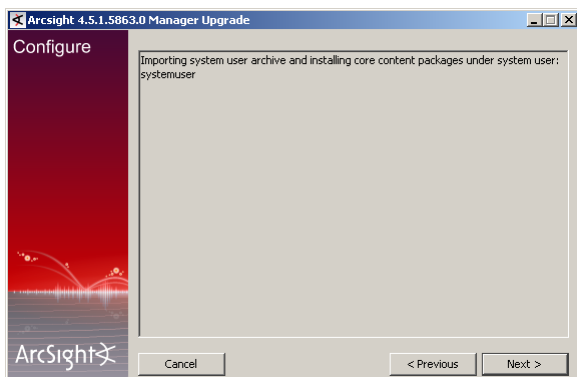
The modification of System Core content can adversely impact the operation of ArcSight ESM, therefore, it is locked by default. ArcSight strongly recommends against unlocking or modifying this content. However, a special user called the system user is created automatically during the installation. This user can lock and unlock ArcSight Core Content if there is a need.

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

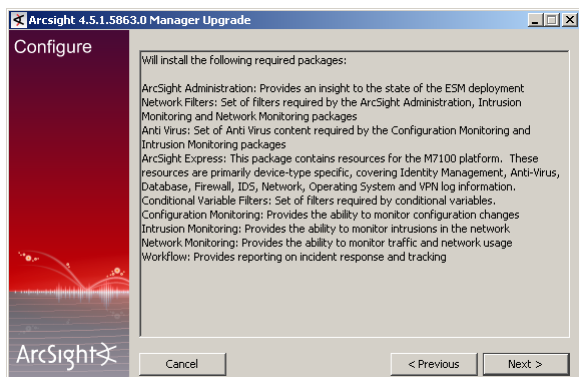
- 14** You will be informed that the ArcSight Foundation Content packages will be installed under user admin. This is the user that will own the Foundation content. Click **Next**:



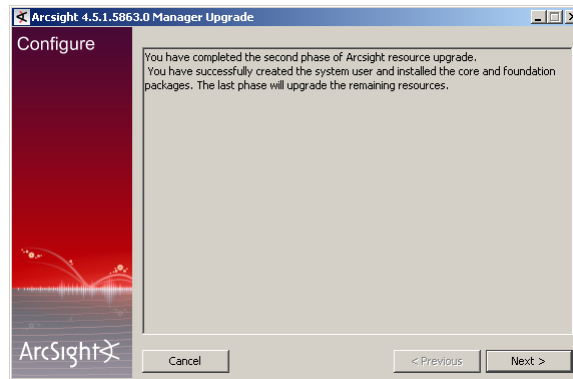
- 15** You will be informed that the core content packages will be installed under systemuser. Click **Next**:



- 16** Next the installer installs the required packages:



- 17 You will see the following screen when the content installation completes:



- 18 Resource Validation is a feature that allows you to automatically validate a resource. Some of the checks done are:

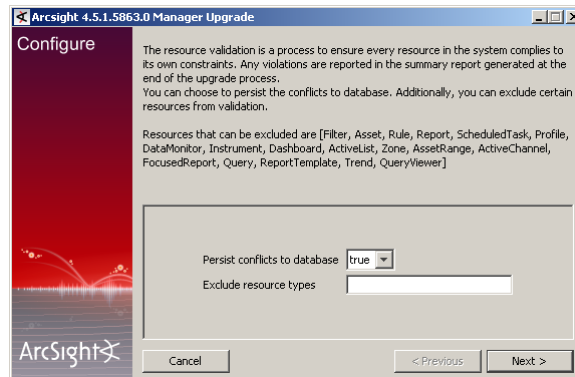
- ◆ Does a resource have valid values assigned to it?
For example, the validation process checks if an IP address assigned to an asset falls in the range of IP address assigned to the zone to which the asset belongs. If the IP address is outside the range, this discrepancy is listed in a report that is generated at the end of the upgrade process.
- ◆ Does the resource satisfy its referential integrity?
For example, a rule depends on filters A, B, and C. If any of these filters is missing, the validation process will detect it and report it at the end of the upgrade process.

You can choose to mark a resource invalid (that is, disabled) if it does not meet all of the checks performed on it. Or you may choose to obtain a report of all such resources and fix them manually.

When a resource is marked invalid (that is, disabled), it is not used to evaluate events, trends, reports, data monitors, or channels in real time. For example, if an asset is marked invalid, it can not participate in the event asset resolution. As a result, correlated events in which the source or target address points to the invalid (disabled) asset are not generated. Similarly, if a rule is marked invalid (disabled), it does not get triggered; therefore, the corresponding correlation events are not generated.

If you set **Persist conflicts to database** to false, the resources that do not meet all of the checks are reported but not marked invalid. But, if you set **Persist conflicts to database** to true, the resources are reported and marked invalid in the database.

You can exclude certain resources from being validated. To do so, list the resources in the **Exclude resource types** field in the following screenshot.

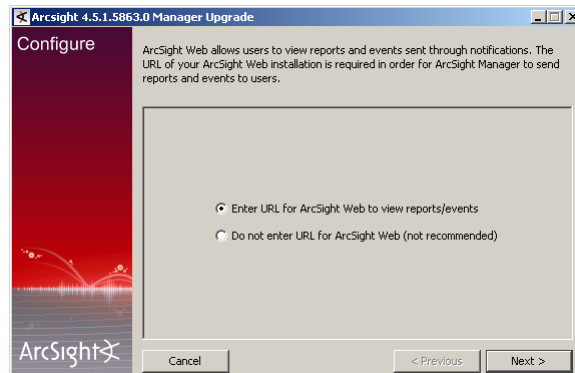


You can validate resources at any time. For example, you may want to revalidate your system after upgrade has completed.

To validate resources at any time, run this command in your Manager's `ARCSIGHT_HOME/bin` directory:

```
arcsight resvalidate -persist [true | false] -excludeTypes
<list of comma-delimited resource types>
```

- 19** If you had an ArcSight Web server set up for your v4.0 SP3 installation or you want to set up an ArcSight Web server for v4.5 SP1, select **Enter a URL for ArcSight Web to view report/events** and click **Next** in the following screen:

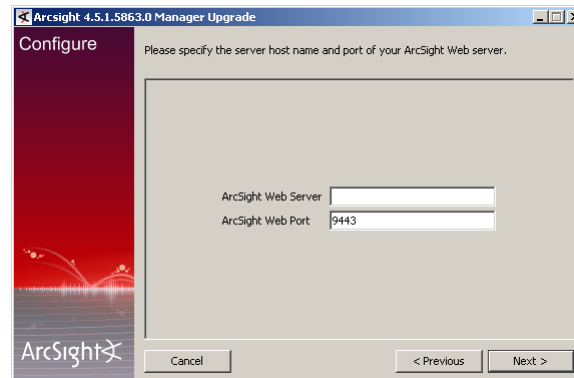


If you did not have an ArcSight Web server set up for v4.0 SP3 and do not want to set up one for v4.5 SP1, select **Do not enter URL for ArcSight Web** and click **Next**.

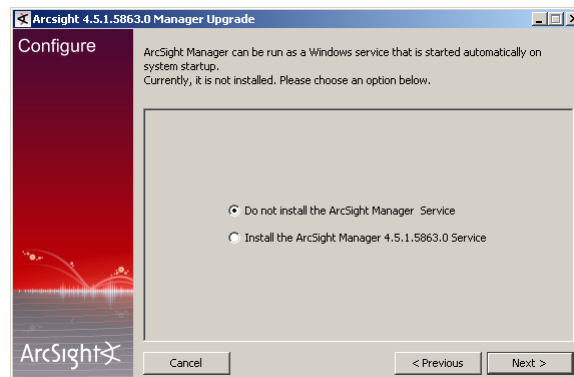
- 20** If you are setting up an ArcSight Web server for v4.5 SP1, enter this information in the following screen:

- ◆ **ArcSight Web Server**—Host name of the machine on which your ArcSight Web is installed.

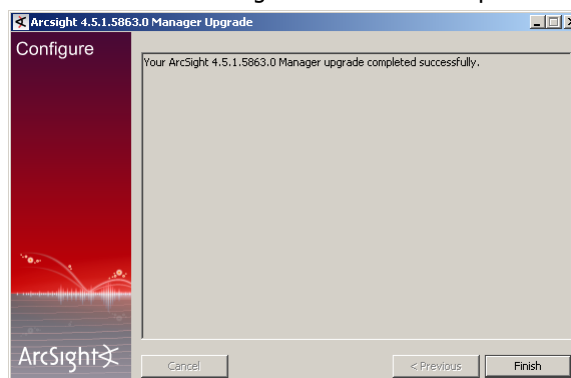
- ◆ **ArcSight Web Port**—Port number on which it listens for connections from ArcSight Web browser clients. (By default, 9443.)



- 21 The option you select from these Manager startup options will take effect when the Manager machine reboots:



- 22 On Unix platforms, if you get a message saying changes to the service configuration require root privileges, follow the steps listed in the message.
- 23 During the upgrade, the v4.0 SP3 `config/server/agentURLMapping.csv` file is saved with the file extension `.previous` in the `config/server` directory of v4.5 SP1 `ARCSIGHT_HOME`. If you customized this file in v4.0 SP3 and want to use it for v4.5 SP1, rename the saved file to remove the `.previous` extension. That is, rename `agentURLMapping.csv.previous` to `agentURLMapping.csv`.
- 24 You will see this message on successful completion of the upgrade:

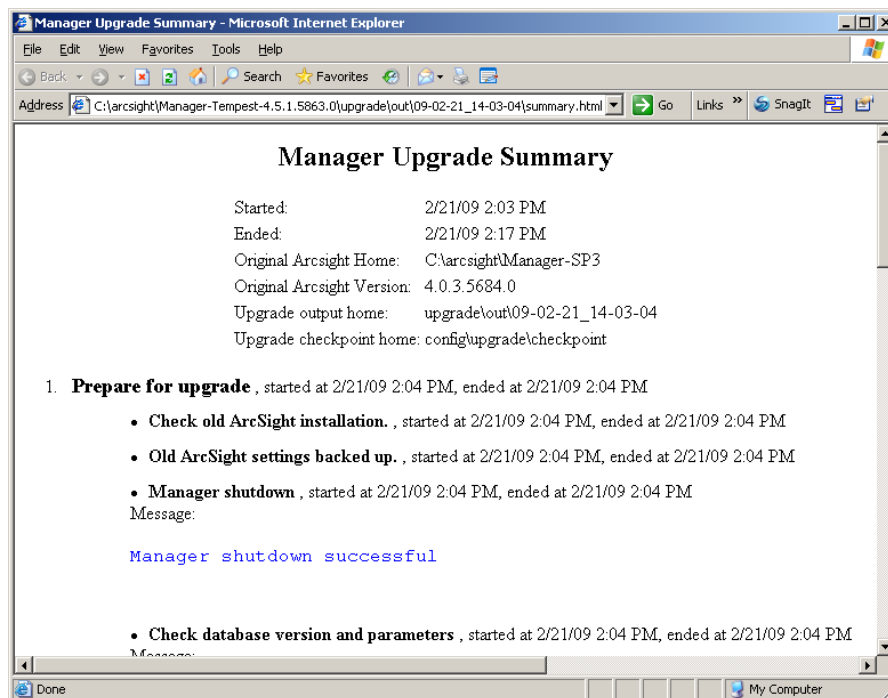


- 25 A summary report is generated at the end of the upgrade process. It lists the outcome of various processes and checks that were run during the upgrade. In some cases, the report also guides you to take action, such as manually migrating a file containing

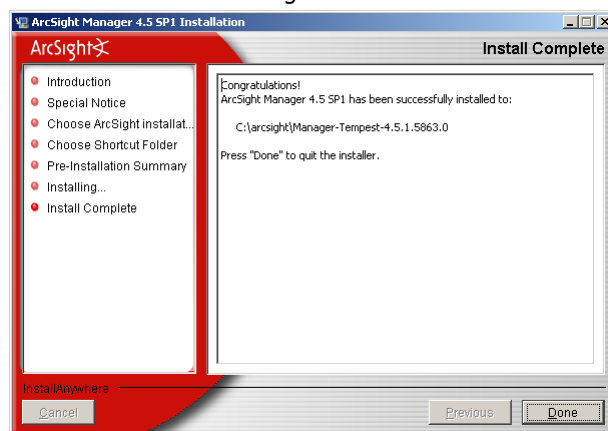
customized content that may not have been moved over from your v4.0 SP3 to the v4.5 SP1 installation or fixing invalid resources.

ArcSight strongly recommends that you review the summary report to ensure that the upgrade was successful. The report is displayed as a pop up at the end of the upgrade process. You can also access the report in ARCSIGHT_HOME/upgrade/out/<time_stamp>/summary.html.

The following screen shows part of an example summary report:



26 Click **Done** in the following screen to exit the wizard:



You have upgraded ArcSight Manager to v4.5 SP1.

27 Start the Manager.

For instructions about starting your ArcSight Manager, see *ArcSight ESM Administrator's Guide, v4.5 SP1*.

Updating and Starting the Partition Archiver Service

If you had Partition Archiver set up in your previous installation, you are required to update and start its service after upgrading ArcSight Manager. These steps are required to upgrade the Partition Archiver version when viewed from the Console. With the Manager running:

- 1 Run the following command from the Database `bin` directory to update the Partition Archiver:

```
arcsight agentsetup -w
```
- 2 Click **Next** on the few wizard screens until you get to the screen which asks you to either review or modify the parameters.
- 3 Select **I do not want to change any settings** and click **Next**.
- 4 Click **Finish** in the last screen.
- 5 Start the Partition Archiver Agent.

◆ **On Windows:**

Open the Service console and start the Partition Archiver Agent service (the default is `Arcsight Oracle Partition Archiver Database`).

◆ **On Solaris, AIX, and Linux:**

Run the following command:

```
/etc/init.d/arc_oraclepartitionarchiver_db start
```



`arc_oraclepartitionarchiver_db` is the default service name.

- 6 For all platforms, check the `logs/agent.out.wrapper.log` file to verify that the Partition Archiver service started successfully. Additionally, verify that the next scheduled partition for archive is archived as expected.

Upgrading ArcSight Consoles

Upgrading ArcSight Consoles

The following platforms are supported for ArcSight Console:

Platform	Supported Operating System	Typical System Requirements
Linux	RHEL v4.0 WS update 7 (32 bit) RHEL v4.0 AS update 7 (64 bit) RHEL v5.3 WS update 2 (32 bit)	x86-compatible
Microsoft Windows	Microsoft Windows Server 2003 R2 SP2 (32-bit and 64-bit) Microsoft Windows Server 2008 (64-bit) Microsoft Windows Vista SP1 (32-bit and 64-bit) Microsoft Windows XP Professional SP3 (32-bit)	x86-compatible
Solaris	Sun Solaris 10 SPARC (64-bit)	Ultra Sparc compatible
Macintosh	Macintosh OS X PPC 10.5.6 (64-bit)	Intel processor



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

Perform the following steps to upgrade one of your ArcSight Consoles to test the upgraded Manager:

- 1 Stop ArcSight Console if it is running.
- 2 If you downloaded the v4.5 SP1 Console installation file to a different machine, transfer it to your Console machine.

- 3 Run the installation file.
- 4 Step through the Installation wizard screens. Specifically, enter values as described below for the following wizard screens:
 - ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v4.5 SP1 that is different from where the existing Console is installed.



Do NOT install v4.5 SP1 Console in the same location as the existing Console.

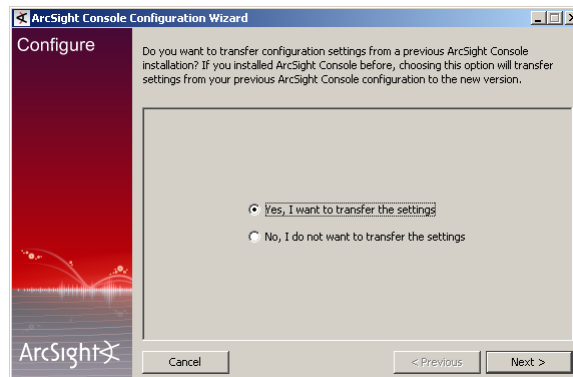
Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder (on Windows)/Choose Link Folder (on UNIX)**—Specify or select where the ArcSight Console icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.
- ◆ **Pre-Installation Summary**—Review the settings and click **Next**.

After you have stepped through the Installation Wizard, it automatically starts the Configuration Wizard.

- 5 The Console installation program detects a previous installation and provides you an option to copy your existing settings to the new Console. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type.

Copying existing settings is optional.



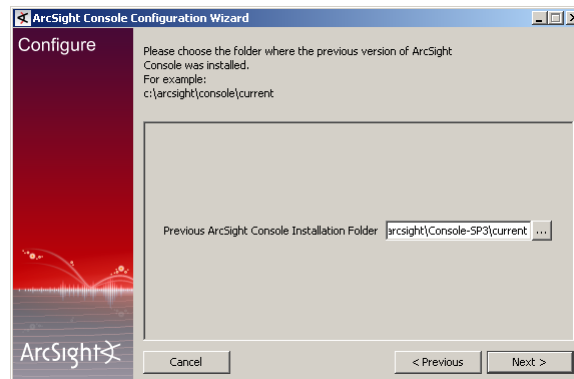
In FIPS mode only: When upgrading the Console, if you select **Yes, I want to transfer the settings** option, you will see the following error:

Problem checking for the demo CA certificate in
`/tmp/Console/current /config/keystore.tempca.`

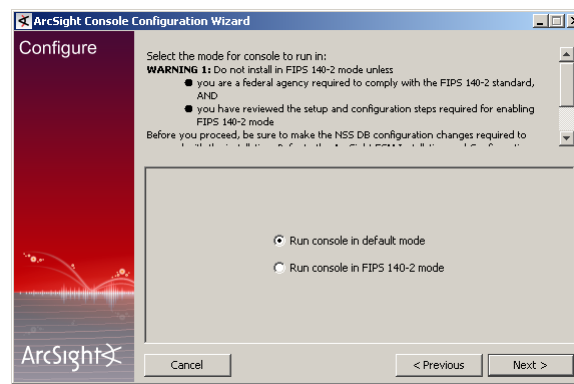
This is because `nssdb.client` does not get copied to the new installation.

Workaround: Manually copy `<ARCSIGHT_HOME>/config/nssdb.client` from your v4.0 SP3 installation to the corresponding location in your v4.5 SP1 installation.

- 6 You will be prompted to enter the location of your previous Console installation:



- 7 In the following screen, select the mode in which you want to upgrade and click **Next**:



- 8 See the *ArcSight ESM Installation and Configuration Guide, v4.5 SP1* for details on the remaining screens for installing a Console using the installation wizard.

- 9 Start the ArcSight Console.

A What's new Quick Start screen is displayed automatically. This screen summarizes the new features in ESM v4.5.

- 10 After you have upgraded a Console to v4.5 SP1, make sure:

- a You can view the upgraded standard content
- b All SmartConnectors you noted in the preparatory step for Manager upgrade are connecting to the Manager.
- c The Manager is receiving events from the SmartConnectors.

If no event viewers appear initially in the Console, select the [All Active Channels/ArcSight System/Core/Live](#) channel to view real-time events.

- 11 If you are able to test the Manager for a successful upgrade using one Console, repeat this procedure to upgrade the remaining Consoles (if any).

If you are not able to test the Manager for a successful upgrade, contact Arcsight Customer Support.

Chapter 5

Upgrading ArcSight Web

Upgrading ArcSight Web



The list of supported platforms for ArcSight Web v4.5 SP1 is same as the one for ArcSight Manager v4.5 SP1.

The following web browsers are supported in this release:

Browser	Version
Internet Explorer on Windows	6.0, 7.0
Safari on Macintosh OS X	2.0, 3.1
Firefox on Windows	2.0, 3.0
Firefox on Linux	2.0, 3.0
Firefox on Solaris SPARC	1.5
Firefox on Macintosh OS	2.0, 3.0

Perform the following steps to upgrade your ArcSight Web.

- 1 Make sure that your Manager is up and running.
- 2 Stop ArcSight Web if it is running.
- 3 If you downloaded the v4.5 SP1 ArcSight Web installation file to a different machine, transfer it to your ArcSight Web machine.
- 4 Run the installation file.
- 5 Step through the Installation Wizard screens. Specifically, enter values as described below for the following Wizard screens:
 - ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v4.5 SP1 that is different from where the existing Web is installed.



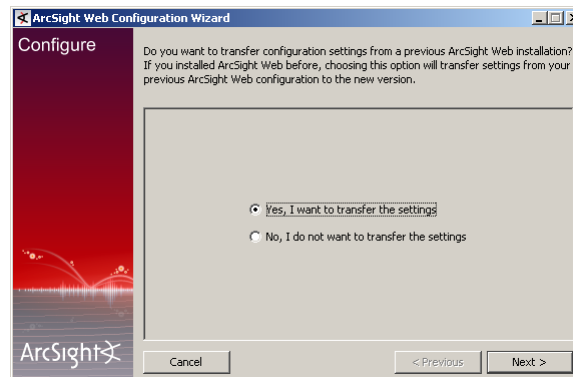
Do NOT install v4.5 SP1 Web in the same location as the existing Web. Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder (on Windows)/Choose Link Folder (on UNIX)**—Specify or select where the ArcSight Web icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.
- ◆ **Pre-Installation Summary**—Review the settings and click **Next**.

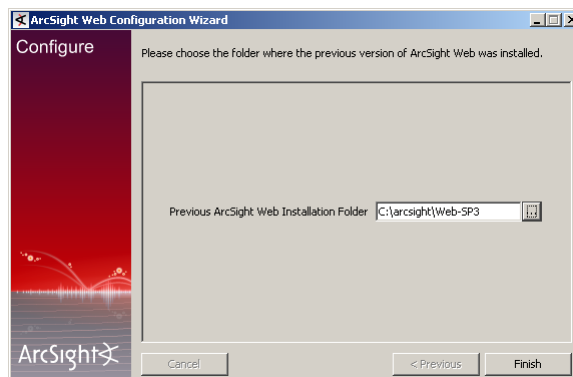
After you have stepped through the Installation wizard, it automatically starts the Configuration wizard.

- 6 The Web installation program detects a previous installation and provides you an option to copy your existing settings to the new Web. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type.

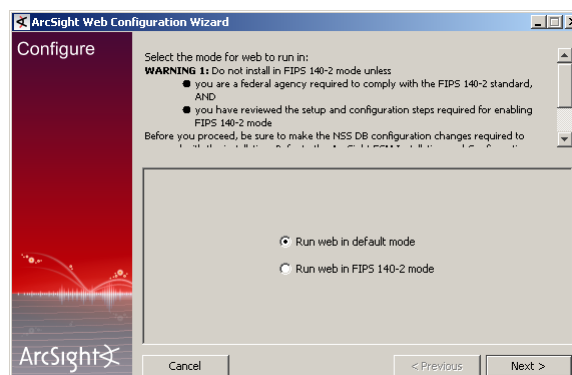
Copying existing settings is optional.



- 7 The Web installation program detects a previous installation.



- 8 Running Web in FIPS mode is not supported for this release. In the following screen, make sure that you select **Run web in default mode** option and click **Next**:



9 When prompted to set the Java Heap Size, make sure to set it to the heap size you had set in your previous ArcSight Web installation.

10 Continue with the upgrade by following in the instructions on the screens.

See the *ArcSight ESM Installation and Configuration Guide, v4.5 SP1* if you need help on any screen for installing ArcSight Web using the installation wizard.

Upgrading ArcSight SmartConnectors

At a minimum, the SmartConnectors must be running version 4021. However, ArcSight strongly recommends that you upgrade all connectors to the latest available release. If you have a setup in the US time zone, we recommend that you run SmartConnector release 4785 or above in order to avoid DST-related issues. Refer to the DST documents provided on the ArcSight Support download site for details.

Perform the following steps to upgrade SmartConnectors:

- 1** Identify all SmartConnectors that you will upgrade.
- 2** If you downloaded the SmartConnector installation file on a different machine, transfer it to your SmartConnector machine.
- 3** Run the SmartConnector installation file.
- 4** Follow the installation wizard screens to upgrade your SmartConnector.
- 5** Repeat [Step 3](#) and [Step 4](#) for every SmartConnector you identified in [Step 1](#).

ArcSight ESM provides the ability to upgrade the SmartConnectors remotely using the [.aup](#) file. For detailed instructions on how to upgrade SmartConnectors remotely, see the *SmartConnector User's Guide*.

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.

Checking the State of Existing Content After Upgrade

After the upgrade is complete, do the following checks to verify that all your content has been successfully transferred to the v4.5 SP1 structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

- **Check for Unassigned resources.** After the upgrade, check the Unassigned group in the resource tree for all resource types. The Unassigned groups in each resource type contain any customer-created resources that were located in a v4.0 SP3 *System* group.

If you find resources in them, move them to other groups, as appropriate. ArcSight recommends against moving these resources into ArcSight standard content groups, as they will be moved to the Unassigned group again when future upgrades occur.

- **Restore customizations to resources with the original resource IDs.** If you had custom configurations to any resource with an original ArcSight resource ID, restore your configurations manually after upgrade is complete from the backed up version you saved before upgrade.
- **Assets Resource.** The Disabled group in the assets resource tree is dynamic, which means it queries the Manager every two minutes for assets that have been disabled. After upgrade, check to see if any assets were disabled and moved to the Disabled group in the Assets resource tree.
 - ◆ If so, review the disabled asset to see the reason it was disabled and fix it as appropriate. For example, if an asset's IP address is outside the range of the upgraded zone, either expand the range of the zone, or assign the asset to another zone.
 - ◆ You can also delete an asset that has become disabled if it is no longer needed (right-click the asset and select **Delete**).
- **Users Resource.** Only the system user has access privileges to the [/All Users](#) resource tree. Therefore, any users or groups you created in [/All Users](#) in the previous installation are now available under [Custom User Groups](#).

After upgrade, verify that your user ACLs are correct and still valid based on how ArcSight standard content is organized for v4.5 SP1. For example, Administrator access should only be granted to those with authority to work with system-level content, such as ArcSight System and ArcSight Administration. Update user ACLs manually as appropriate.
- **Zones Resource.** Check to see if any zones were invalidated during the upgrade process.
 - ◆ Fix zones that may have become invalid during upgrade that you want to keep.

- ◆ Verify that the assets assigned to zones that have been moved or invalidated during the upgrade retain their connections to the appropriate v4.0 SP3 zones.
- ◆ Delete any invalid zones that you no longer want to keep.
- ◆ If you made customizations to the standard v4.0 SP3 zones, manually edit the new resource to restore the customizations you made to the v4.0 SP3 zone. Do not import the old zone.
- **Repair any invalid resources.** During the upgrade process, the resource validator identifies any resources that are rendered invalid (conditions that no longer work) during the upgrade. Review the upgrade summary report in [ARCSIGHT_HOME/upgrade/out/<time_stamp>/summary.html](#) to find invalid resources and fix their conditions as appropriate.
- This bullet item applies to you only if you are upgrading from v3.5 SP2 all the way to v4.5 SP1 (that is, if your ESM was upgraded from v3.5 SP2 to v4.0 SP1, and later upgraded to v4.0 SP3, and lastly to v4.5 SP1.)

The data type used for case stage has been updated to be of enumeration data type instead of the String data type used in previous ESM releases. So, if you had Case queries in your system that used string operators on the Case Stage field (for example "stage startsWith 'F'"), you will be required to manually fix those conditions to use operators valid on enumeration data types. For example, if you have a condition "stage startsWith 'F'" and there are two possible enumeration values (2, Final) and (5, Follow-up), you should change the condition to "stage = Final or stage = Follow-up".
- **Verify that customer-created content still works as expected.**

Customer-created content that refers to ArcSight standard content and has been significantly changed may not work as expected.

For example, if you have a rule that uses an ArcSight System filter whose conditions have been changed such that rule matches more events than you expect, or doesn't match the events you expect. Another example is a moving average data monitor whose threshold has been changed.

To verify that the resources you rely upon work as expected, go through the following checks:

 - ◆ Send events that you know should trigger the content through the system using the Replay with Rules feature. For more information about this feature and how it's been enhanced for v4.5 SP1, see the online Help topic *Verifying Rules with Events*.
 - ◆ Check the Live or All Events active channel to verify if the correlation event is triggered, and check that data monitors you created are returning the expected output based on the test events you send through.
 - ◆ Verify that notifications are sent to the recipients in your notification destinations as expected.
 - ◆ Check that any lists you have created to support your content are gathering the replay with rules data as expected.

Index

D

downloading

 Console files 3

 Database files 2

 Manager files 3

 SmaratConnector files 2

 Web files 3

downloading files 2

H

hierarchical manager

 upgrade 1

O

Oracle

 upgrading 12

Oracle files 2

R

Related documentation 4

U

upgrade

 hierarchical manager 1

 preparing for 1

 steps 1

upgrading

 Oracle 9i to 10g 12

