

# Upgrading ArcSight™ ESM

---

v5.0 to v5.0 SP1

January, 2011



## Upgrading ArcSight™ ESM v5.0 to v5.0 SP1

Copyright © 2011 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                          |
|-------|------------------------|--------------------------------------|
| 1/611 | Upgrading ArcSight ESM | v5.0 GA and v5.0 Patch 1 to v5.0 SP1 |

Document template version: 1.0.2.7

## ArcSight Customer Support

|                         |   |
|-------------------------|---|
| <b>Phone</b>            | 1-866-535-3285 (North America)<br>+44 (0)870 141 7487 (EMEA)                                |
| <b>E-mail</b>           | <a href="mailto:support@arcsight.com">support@arcsight.com</a>                              |
| <b>Support Web Site</b> | <a href="http://www.arcsight.com/supportportal/">http://www.arcsight.com/supportportal/</a> |
| <b>Customer Forum</b>   | <a href="https://forum.arcsight.com">https://forum.arcsight.com</a>                         |

# Contents

---

|  |           |
|--|-----------|
| <b>Chapter 1: Preparing for Upgrade .....</b>                                | <b>1</b>  |
| Document Status .....  | 1         |
| Summary .....  | 1         |
| Check for Deprecated Oracle Parameter .....                                  | 2         |
| Downloading Installation Files, Scripts, and Other Documents .....           | 2         |
| <b>Chapter 2: Upgrading ArcSight Database Components .....</b>               | <b>5</b>  |
| Preparing the ArcSight Database Components .....                             | 5         |
| Upgrading the ArcSight Database Software, and Partition Archiver .....       | 7         |
| Transferring Partition Archiver Settings .....                               | 10        |
| <b>Chapter 3: Upgrading ArcSight Manager .....</b>                           | <b>13</b> |
| Preparing the ArcSight Manager .....   | 13        |
| Upgrading the ArcSight Manager .....   | 16        |
| Post-Upgrade Tasks .....   | 25        |
| Upgrading the Index .....  | 26        |
| Updating and Starting the Partition Archiver Service .....                   | 27        |
| <b>Chapter 4: Upgrading ArcSight Consoles .....</b>                          | <b>29</b> |
| Upgrading ArcSight Consoles .....  | 29        |
| <b>Chapter 5: Upgrading ArcSight Web .....</b>                               | <b>33</b> |
| Upgrading ArcSight Web .....   | 33        |
| <b>Chapter 6: Checking the State of Existing Content After Upgrade .....</b> | <b>37</b> |
| <b>Chapter 7: Upgrading ArcSight SmartConnectors .....</b>                   | <b>39</b> |
| <b>Chapter 8: Upgrading Oracle Database to 11g .....</b>                     | <b>41</b> |
| Required Oracle Packages .....   | 41        |
| On 32-bit Linux: .....   | 41        |
| On Red Hat Enterprise Linux 5 .....  | 41        |
| On 64-bit Linux: .....   | 42        |
| On Red Hat Enterprise Linux 5 .....  | 42        |
| Upgrading Oracle .....   | 42        |

---

|  |           |
|--|-----------|
| Upgrading Oracle 10g Software to 11g .....   | 42        |
| Upgrading a 10g Oracle Instance to 11g ..... | 45        |
| <b>Index .....</b>                           | <b>49</b> |

# Chapter 1

## Preparing for Upgrade

---

### Document Status

This technical note describes the steps required to upgrade the ArcSight ESM from v5.0 GA and v5.0 Patch 1 to v5.0 SP1.



Caution

To have the option to fallback to the previous version, take a full cold-backup of your database installation.

For all components, upgrading is currently supported from FIPS mode to FIPS mode and default mode to default mode only. Upgrading from an existing FIPS mode installation to default mode or vice versa is not supported.

### Summary

Upgrading ArcSight ESM involves the following steps:

[Check for Deprecated Oracle Parameter](#)

[Downloading Installation Files, Scripts, and Other Documents](#)

[Upgrading ArcSight Database Components](#)

[Upgrading ArcSight Manager](#)

[Upgrading ArcSight Consoles](#)

[Upgrading ArcSight Web](#)

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

[Upgrading ArcSight SmartConnectors](#)

[Upgrading Oracle Database to 11g](#)



Tip

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.

## Check for Deprecated Oracle Parameter

If the version of Oracle you are upgrading has these two characteristics:

- You created the instance using the XXLarge template, and
- You used a version of the ArcSight ESM software earlier than 5.0 GA

You might encounter a problem during the upgrade to Oracle 11g.

- To check whether there is an issue, Run the following commands while logged in as the oracle user (`su -oracle`):

```
% arcdbutil sql
Enter user-name: / as sysdba
sql> show parameter parallel_automatic_tuning
```

If this parameter is set to `TRUE`, then you have an issue, as this parameter is deprecated. Contact ArcSight Technical Support for information on how to eliminate the deprecated parameter from the Oracle parameter file.

## 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 the v5.0 SP1 files for all components on their respective machines. Refer to the ESM v5.0 SP1 Release Notes for the file names and locations.
- Download files directly to the component machines where they will be installed.

### For the SmartConnectors:

Download installation files as appropriate for your SmartConnector platforms. To leverage the ESM v5.0 schema, you will need to use SmartConnector version 4.8.1 at a minimum. Use the `.aup` file 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 v5.0 Console, click **Help | About**. The current version is displayed in 5.0.0.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-5.0.1.xxxx.0-DB-Win.exe](#)
- ◆ [ArcSight-5.0.1.xxxx.0-DB-AIX.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-DB-Linux.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-DB-Solaris.bin](#)

#### For the Manager:

- 1 Check the current ArcSight ESM version you are running on the Manager. To check the version, in a v5.0 Console that connects to the Manager, click **Help | About**. The current version is displayed in 5.0.0.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-5.0.1.xxxx.0-Manager-Win.exe](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Manager-Win64.exe](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Manager-AIX.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Manager-Linux.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Manager-Linux64.bin](#)
- ◆ [ArcSight-5.0.1.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-5.0.1.xxxx.0-Console-Win.exe](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Console-Linux.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Console-MacOSX.bin](#)
- ◆ [ArcSight-5.0.1.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-5.0.1.xxxx.0-Web-Win.exe](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Web-AIX.bin](#)
- ◆ [ArcSight-5.0.1.xxxx.0-Web-Linux.bin](#)
- ◆ [ArcSight-5.0.1.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 v5.0 SP1 Release Notes](#)
- [ArcSight ESM Installation and Configuration Guide](#)
- [ArcSight ESM Administrator's Guide](#)
- [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.



## Chapter 2

# Upgrading ArcSight Database Components

---

This chapter is about preparing the ArcSight database components for version 5.0 SP1. After you complete these steps:

- Upgrade the Manager, as described in [Chapter 3, Upgrading ArcSight Manager, on page 13](#).
- Optionally, if you are on a system that supports it, you can upgrade the Oracle database to version 11g, as described in [Chapter 8, Upgrading Oracle Database to 11g, on page 41](#).

## Preparing the ArcSight Database Components

Before you start the upgrade, prepare your ArcSight Database components as follows:

- 1 Verify that your database machine and version is supported. The following table lists the database machines and versions supported for v5.0 SP1.

| Operating System                              | Database                           | Typical System Configuration                     |
|---|------------------------------------|--|
| Microsoft Windows Server 2003 R2 (SP2) 32-bit | Oracle 10.2.0.4<br>Oracle 11.2.0.1 | x86-compatible multi-CPU system with 2-16 GB RAM |
| Microsoft Windows Server 2003 R2 (SP2) 64-bit | Oracle 10.2.0.4<br>Oracle 11.2.0.1 |  |
| Microsoft Windows Server 2008 (SP2) 64-bit    | Oracle 10.2.0.4<br>Oracle 11.2.0.1 |  |

| Operating System                                  | Database                           | Typical System Configuration                       |
|---|------------------------------------|--|
| Red Hat Enterprise Linux 4.0 AS 32-bit update 8   | Oracle 10.2.0.4                    | x86-compatible multi-CPU system with 2-16 GB RAM   |
| Red Hat Enterprise Linux 4.0 AS 64-bit update 8   | Oracle 10.2.0.4                    |  |
| Red Hat Enterprise Linux 5 (RHEL 5.4) AS 32-bit   | Oracle 10.2.0.4<br>Oracle 11.2.0.2 |  |
| Red Hat Enterprise Linux 5 (RHEL 5.4) AS 64-bit   | Oracle 10.2.0.4<br>Oracle 11.2.0.2 |  |
| SUSE Linux 10 SP2 Enterprise Server 64-bit        | Oracle 10.2.0.4                    |  |
| SUSE Linux 11 Enterprise Server 64-bit            | Oracle 10.2.0.4                    |  |
| 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 pSeries | Oracle 10.2.0.4                    | pSeries system with 2-16 GB RAM                    |



Note

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

- 2 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.
- 3 Perform these steps to identify if your v5.0 GA database is ready for upgrade:
  - a Shut down your currently installed v5.0 GA ArcSight Manager.  
For instructions about shutting down your ArcSight Manager, see *ArcSight ESM Administrator's Guide*.
  - b In `ARCSIGHT_HOME/bin` of your v5.0 GA database installation, run the following command:
 

```
./arcsight dbcheck
```

You will see the following files in the Database's `<ARCSIGHT_HOME>/logs/dbcheck` directory:

    - `DatabaseInfo.htm`
    - `EventIndexInfo.htm`
    - `TablespaceInfo.htm`
    - `TableStatsInfo.htm`

- [PartitionInfoV40.htm](#)
- [PartitionStatsInfo.htm](#)
- [ResourceCountV40.htm](#)
- [index.htm](#)

To view a log file, open the [index.html](#) file 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.

- 4 Pre-v5.0 GA archived partitions with archive type uncompressed should not be in reactivated state during Manager upgrade. Deactivate such partitions before you do the Manager upgrade.

## Upgrading the ArcSight Database Software, and Partition Archiver



Even if you choose to use your pre-existing Oracle 10.2.0.4 installation, you must upgrade your ArcSight database software to v5.0 SP1.

- 1 Make sure to close any open connections to Oracle database before proceeding further.
- 2 If you downloaded the v5.0 SP1 ArcSight Database installation file on a different machine, transfer it to your Database machine.
- 3 If you have Partition Archiver service running on your database machine, shut it down.
- 4 Log in as "root" on Unix and "Administrator" on Windows on the database server.
- 5 Run the database installation executable appropriate for your platform:

◆ **On Windows:**

Double-click [ArcSight-5.0.1.xxxx.0-DB-Win.exe](#)

◆ **On Solaris:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-DB-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-DB-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-DB-AIX.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-DB-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

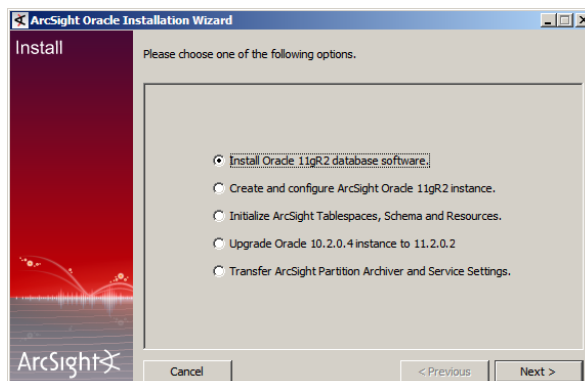
```
./ArcSight-5.0.1.xxxx.0-DB-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

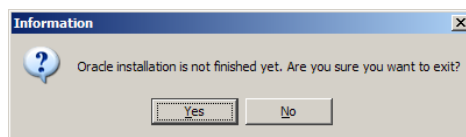
```
./ArcSight-5.0.1.xxxx.0-DB-Linux.bin -i console
```

The installer launches the Introduction window.

- 6 Click **Next** in the Introduction screen.
- 7 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 will be disabled until you scroll to the bottom of the agreement to help ensure that you have read the agreement.
- 8 Read the Special Notice and click **Next**.
- 9 Enter the location where you want to install the v5.0 SP1 database software. This location should be different from the location where you have the v5.0 GA database software installed. Click **Next**.
- 10 Step through the following screens:
  - ◆ **Choose Link Folder** (On Unix) or **Choose Shortcut Folder** (On Windows). 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. Click **Next**.
  - ◆ **Pre-Installation Summary**—Review the pre-installation summary and click **Install**.
- 11 Select an option in the following screen to suit your needs based on the description below and click **Next**.



- ◆ If you did not have Partition Archiver configured in v5.0 GA, click **Cancel** and click **Yes** in the following message box:



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



On Unix systems, the panels are reversed. You will first see the Install complete panel and after you click Done in the panel you will see the configuration screen shown at the beginning of this step.

- ◆ If you have Partition Archiver configured in v5.0 GA, you will need to transfer the Partition Archiver settings to your v5.0 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.



#### 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 v5.0 SP1. See the section, ["Updating and Starting the Partition Archiver Service" on page 27](#) in the [Upgrading ArcSight Manager](#) chapter.
- If you have pre-v5.0 archived partitions and you had set up your Partition Archiver to archive with type uncompressed, backup your archive folder (that contains partition that you are trying to reactivate) before reactivation.

Keep in mind that if/when you reactivate the partition, the reactivation of the partition will succeed if there is only one data file (.dbf file) present for that partition.

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 while logged in as the oracle user (`su -oracle`):

```
% arcdbutil sql

Enter user-name: / as sysdba

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

#### Optional:

Run the following command while logged in as the Oracle user (`su -oracle`) 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
```

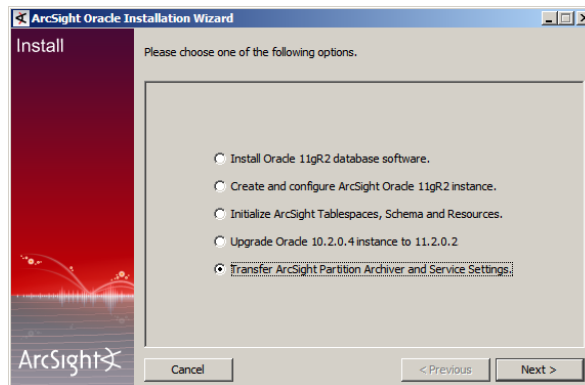


This script should be run every time you make any storage hardware changes that affects IO transfer speeds.

You have upgraded the ArcSight Database v5.0 SP1 software. Go to the next section [Upgrading ArcSight Manager](#).

## Transferring Partition Archiver Settings

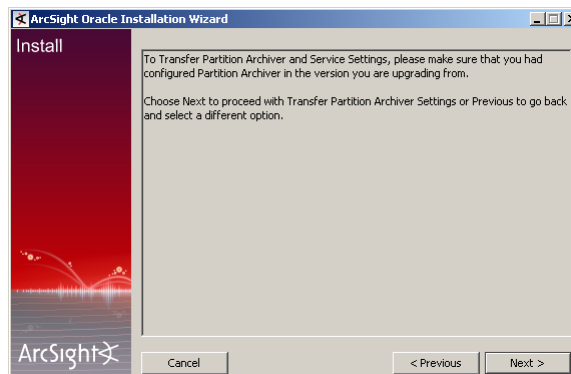
- 1 Select the **Transfer ArcSight Partition Archiver and Service Settings** option as shown and click **Next**:



**Note**

The screen shots in this guide that show 11.2.0.2 will show 11.2.0.1 when you are installing Windows.

- 2 Click **Next** to confirm that you had configured the Partition Archiver in v5.0 GA:

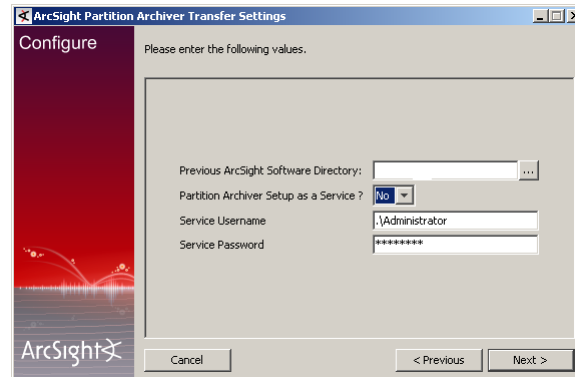


- 3 Enter the path name of the existing ArcSight Database's `<ARCSIGHT_HOME>` and

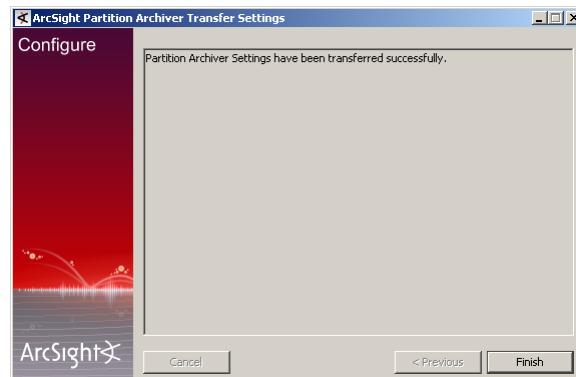
**On Windows Only:** Also enter your Windows Administrator's user name and password.

If you had set up the Partition Archiver as a service in your previous installation, select **Yes** from the **Partition Archiver as a service?** drop-down list, otherwise select **No**.

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 v5.0 GA Database installation.

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





## 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 v5.0 SP1 from the list of supported platforms and database versions in ["Preparing the ArcSight Database Components" on page 5](#).
- 2 Verify that your Manager machine is supported for v5.0 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. On a 32-bit platform, use 32-bit installer.

| Platform | Supported Operating System                               | Typical System Requirements                     |
|----------|--|---|
| Linux    | Red Hat Enterprise Linux 4.0 (RHEL 4) AS 32-bit update 8 | x86-compatible multi-CPU system with 2-4 GB RAM |
|          | Red Hat Enterprise Linux 4.0 (RHEL 4) AS 64-bit update 8 |   |
|          | Red Hat Enterprise Linux (RHEL 5.4) 32-bit               |   |
|          | Red Hat Enterprise Linux (RHEL 5.4) 64-bit               |   |
|          | SUSE Linux 10 SP2 Enterprise Server 64-bit               |   |
|          | SUSE Linux 11 Enterprise Server 64-bit                   |   |

| Platform          | Supported Operating System   | Typical System Requirements                       |
|-------------------|--|---|
| Microsoft Windows | Microsoft Windows Server 2003 R2 (SP2) 32-bit<br>Microsoft Windows Server 2003 R2 (SP2) 64-bit<br>Microsoft Windows Server 2008 SP2 32-bit<br>Microsoft Windows Server 2008 SP2 64-bit | x86-compatible multi-CPU system with 2-4 GB RAM   |
| Solaris           | Sun Solaris 10 (10/09) 64-bit  | Sparc-compatible multi-CPU system with 2-4 GB RAM |
| IBM AIX           | IBM AIX 5L, Version 5.3 (5.3.0.70) 64-bit  | pSeries system with 2-16 GB RAM                   |

**Note**

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

- 3** If you downloaded the latest patch for your ArcSight Manager, install it.
- 4** We recommend that you make a note of the details of your customized zones, such as the start and end addresses, their location in the directory hierarchy, etc. It will come handy 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 Components” on page 5. After running `dbcheck`, make sure that all log files the script generates are error and warning free.
- 6** Pre-v5.0 archived partitions with archive type uncompressed should not be in reactivated state during Manager upgrade. Deactivate such partitions before you do the Manager upgrade.
- 7** 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—Set to the directory where Oracle is installed on your system

ORACLE\_SID—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 v5.0 GA 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. For example,

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



**Note**

- Use the `-s` option in this command to export the session list tables too.
- When running the `export_system_tables` command, you may see an warning message in your command prompt or shell console window saying "Exporting questionable statistics". You can safely ignore this warning. This warning occurs when you export the table data with its related optimizer statistics and Oracle cannot verify the validity of these statistics.

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 your v5.0 GA Database's `<ARCSIGHT_HOME>` directory.

- 8** By default, the heap size set for the upgrade process is 1 GB. If you have a large number of resources the upgrade process might need more memory. In such a situation, reset the heap size for the upgrade process to equal the heap size that you had set on your v5.0 GA Manager. To do so,
- a** Run the following command from your v5.0 GA Manager's `\bin` directory:

```
arcsight managersetup
```

- b** Accept all the defaults and click **Next** in the first few screens.
- c** Note the value of the Java Heap Size when you get to the screen.
- d** Set the `ARCSIGHT_JVM_OPTIONS` as follows by substituting the value for the `<manager_heap_size>` with the Java Heap Size value of your v5.0 GA Manager.

**On Windows:**

```
set ARCSIGHT_JVM_OPTIONS=-Xmx<manager_heap_size>m
```

Leave the command prompt window open and go to "Upgrading the ArcSight Manager" on page 16.

**On Unix:**

```
export ARCSIGHT_JVM_OPTIONS=-Xmx<manager_heap_size>m
```

- e** Make sure to run the upgrade from the same command window in which you set the `ARCSIGHT_JVM_OPTIONS`.

## 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 13](#).



In case of a failure during upgrade, be sure to check the log files for errors. Make any configuration changes if necessary per the error in the log file, then restart the upgrade process.

Perform these steps to upgrade your Manager:

- 1 If you downloaded the v5.0 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*.

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

This step is required because the v5.0 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.

◆ **On Windows:**

Double-click `ArcSight-5.0.1.xxxx.0-Manager-Win.exe`

◆ **On Solaris:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Manager-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Manager-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Manager-AIX.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Manager-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Manager-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Manager-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Click **Next** in the Introduction window.
- 6 Step through the Installation wizard screens.

Specifically, enter values as described below for the following wizard screens:

- ◆ **License Agreement**—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**.
- ◆ **Special Notice**—Read the notice and click **Next**.
- ◆ **Choose ArcSight Installation Directory**—Enter an `<ARCSIGHT_HOME>` path for v5.0 GA that is different from where the existing Manager is installed. Click **Next**.



Do NOT install v5.0 SP1 Manager in the same location as the existing Manager.

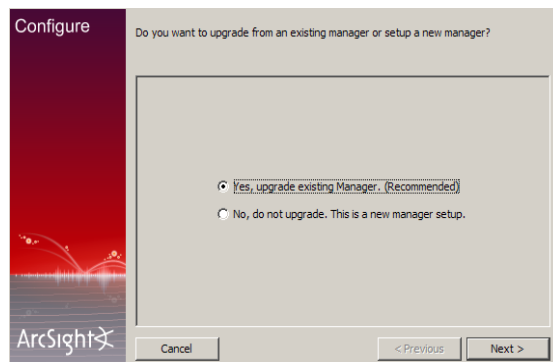
Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder** (on Windows) or **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. Click **Next**.
- ◆ **Pre-Installation Summary**—Review the settings and click **Install**.



On Windows, if you had set the `ARCSIGHT_JVM_OPTIONS` option to your Manager's heap size, you need to cancel out of the screen and run `arcshint upgrade manager` command from the v5.0 SP1 Manager's `\bin` directory in the same command window where you had set the manager's heap size.

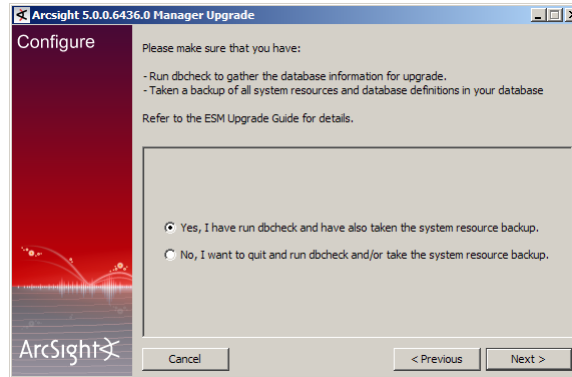
- 7 Select **Yes, upgrade existing Manager. (Recommended)**, and click **Next**.



- 8 You will see a message requesting you to make sure that you have a good understanding of all components before upgrading. Click **Next**.
- 9 If you did not run the `dbcheck` script on your database as described in “Preparing the ArcSight Database Components” on page 5, you must run it and make sure that all log files the script generates are error and warning free. Also, you should have made a

backup of the system dump by this point. If you have not done so yet, do that before continuing with the upgrade.

- ◆ To stop the Manager upgrade at this point, select **No, I want to quit and run dbcheck and/or take the system resource backup** and click **Cancel** in the following screen.

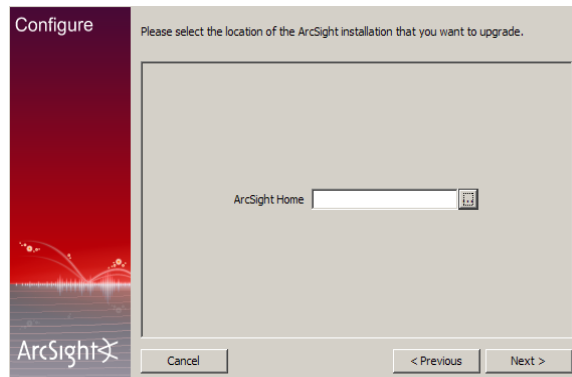


After you have run the `dbcheck` script, you can resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:

```
arcsight upgrade manager
```

The upgrade process resumes from this point.

- ◆ To continue with Manager upgrade, select **Yes, I have run dbcheck and have also taken the system resource backup** and click **Next** in the above screen.
- 10** Select the location of v5.0 GA Manager installation in the following screen and click **Next**:



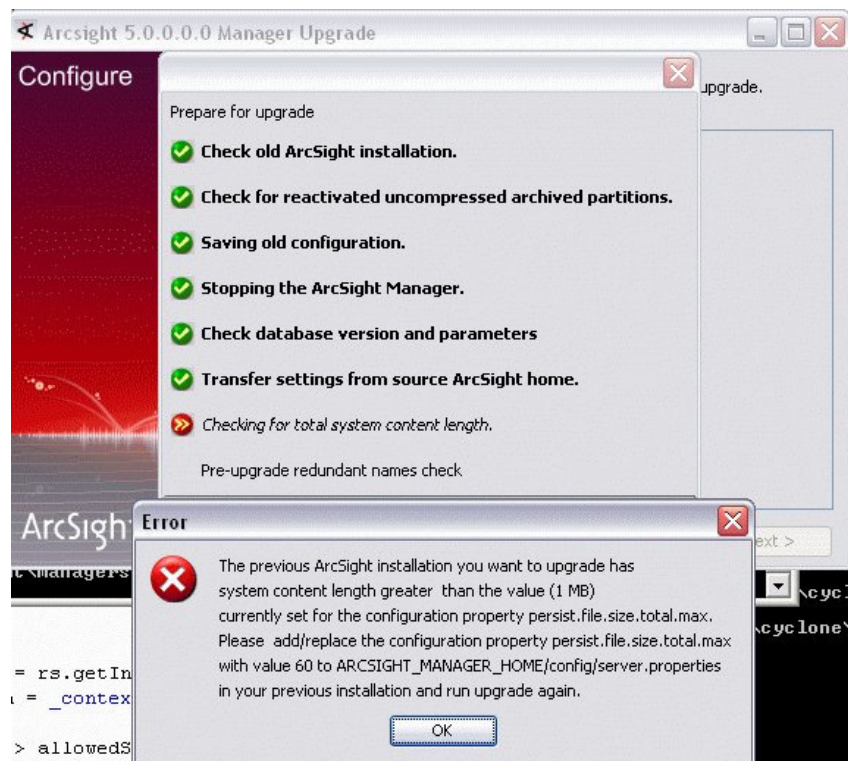
If you see an error asking you to backup your system tables, click **OK** in the error dialog, leave the configuration running, and follow the instructions in [Step on page 14](#). Then go back to wizard and continue to completion.

If you are upgrading from v4.5 SP2 or SP3, on Linux with a French Locale, you might get an error like this:

```
Transfer setting from source ArcSight Home with error "2010-12-15 3:30:32,621] [ERROR]
[default.com.arcsight.upgrade.wizard.ManagerLocationPanel] [processNext] java.io.FileNotFoundException:
/opt/arcsight/45sp3p1/manager/reports/archive/images/image_2Archived_Reports.Meta.Group/Personal_Archived_Reports/admin's_Rapports_archiv??s (No such file or directory)
```

If you get an error like this, use the following workaround procedure:

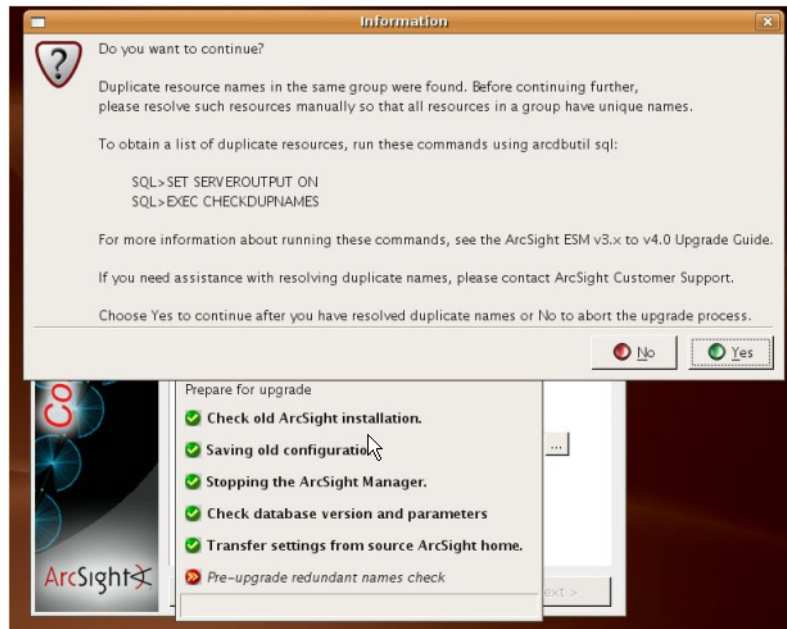
- a** Backup the folder `ARCSIGHT_HOME/Manager/reports/archive`.
  - b** Delete the folder `ARCSIGHT_HOME/Manager/reports/archive`.
  - c** Resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:  
  
`arcsight upgrade manager`
  - d** When you have completed the Manager upgrade to v5.0 SP1, restore the folder `ARCSIGHT_HOME/Manager/reports/archive`.
- 11** If you are not using Oracle 11g, you see a warning message recommending that you upgrade your Oracle database to 11g. You are also asked whether you want to continue with the Manager upgrade. Click **Yes** to continue.
- You can upgrade your Oracle database after you have upgraded all ESM components to v5.0 SP1 and verified that all components have been upgraded successfully.
- 12** The Manager upgrade automatically checks if the current ESM system content length in the database exceeds the maximum length allowed by the `persist.file.size.total` property on the Manager. If so, you get the following error:



The error message provides the increased value that you need to set:

- a** Find the file `<ARCSIGHT_MANAGER_HOME>/config/server.properties` in your previous ArcSight installation.
- b** Add (or replace, if it is already present) the value for `persist.file.size.total.max` using the value recommended in the error message. For example: `persist.file.size.total.max=60`
- c** Save the `server.properties` file.
- d** Restart the Manager upgrade.

- 13** 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 the v5.0 SP1 ArcSight Database installation's `ARCSIGHT_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.



- 14** The upgrade process also checks for pre-v5.0 SP1 archived partitions with archive type uncompressed which are in reactivated state. If you have such partitions, deactivate them before you do the Manager upgrade.
- 15** You will see a message saying that you have completed the first stage of upgrade. Click **Next**.



Note

If the Manager upgrade fails from this point forward, check the logs to see the cause of the failure. Make any configuration changes if necessary and rerun the upgrade process.

If you still get an error, import the v5.0 GA system tables you exported in ["Preparing the ArcSight Manager" on page 13](#) and then rerun:

```
arcsight upgrade manager
```

from the `/bin` directory of the location where you installed the v5.0 SP1 Manager.

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>
```

Make sure to use the absolute path to this file when importing it.

At this point the following takes place:

- ◆ Upgrade system tables to v5.0 SP1
- ◆ Upgrade system indexes to v5.0 SP1
- ◆ Remove undelivered notifications
- ◆ Upgrade user functions

ArcSight's stock content is installed as follows:



Note

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.

#### ◆ System Core content

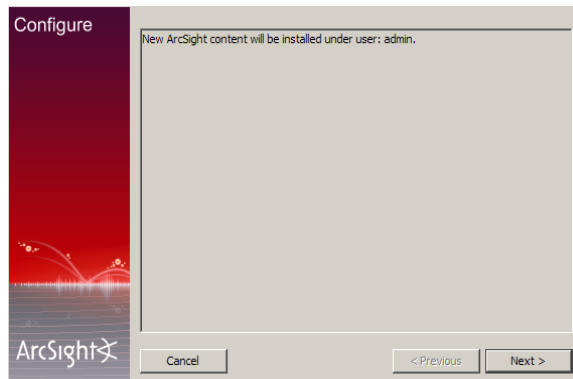
The System Core content provides the foundation building blocks for ArcSight ESM to work. This content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in `/All Filters/ArcSight System/Core`.

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.

#### ◆ 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.

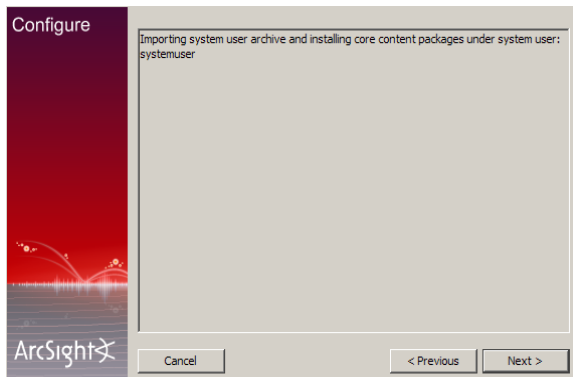
- 16** You will be informed that the ArcSight Content packages will be installed under user admin. This is the user that will own the system content. Click **Next**:



The following takes place:

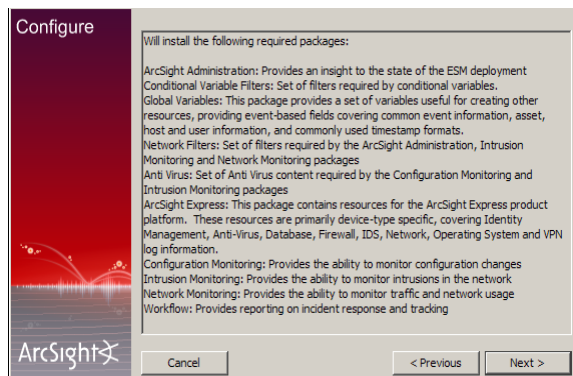
- ◆ Set enough cache size for resources
- ◆ Upgrade ArcSight system content resources

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



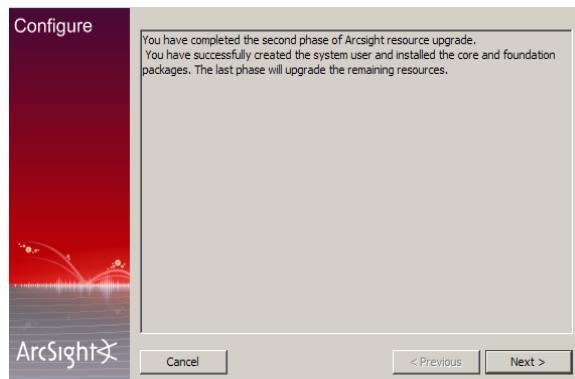
At this point the system user is updated and the core content is installed.

- 18** Next the installer informs you that it will begin installing the required packages (Foundation content):



Click **Next**.

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



Click **Next**.

At this point the following happens:

- ◆ User's personal group upgrade
- ◆ Resource Fix-up
- ◆ Viewer configuration upgrade
- ◆ Update the database schema to the latest version

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

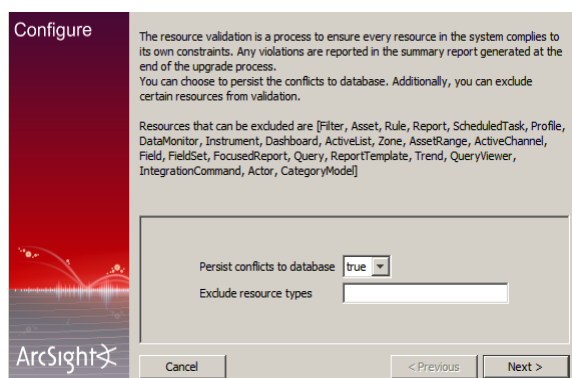
- ◆ Does a resource have valid values assigned to it?  
For example, the validation process checks if an IP address assigned to an asset falls in the range of IP address assigned to the zone to which the asset belongs. If the IP address is outside the range, this discrepancy is listed in a report that 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.



**Tip**

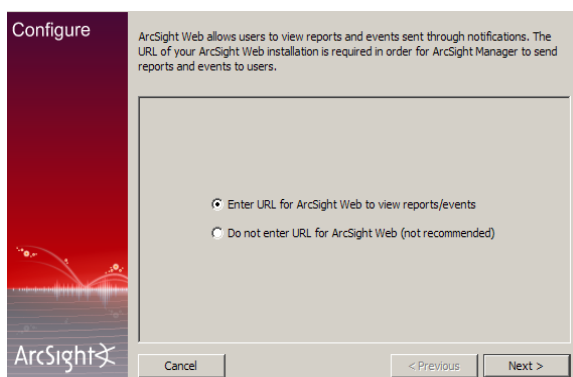
You can validate resources at any time. For example, you may want to revalidate your system after upgrade has completed.

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>
```

You need to have the same `ARCSIGHT_JVM_OPTIONS` as your v5.0 GA Manager when running this. See [Step d on page 15](#) for details on setting `ARCSIGHT_JVM_OPTIONS`.

- 21** If you had an ArcSight Web server set up for your v5.0 GA installation or you want to set up an ArcSight Web server for v5.0 SP1, select **Enter a URL for ArcSight Web to view report/events** and click **Next** in the following screen:

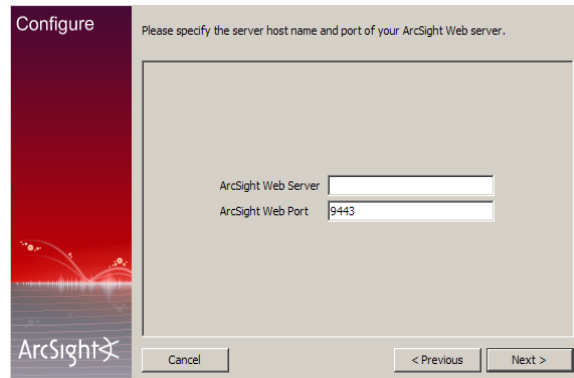


If you did not have an ArcSight Web server set up for v5.0 GA and do not want to set up one for v5.0 SP1, select **Do not enter URL for ArcSight Web** and click **Next**.

- 22** If you are setting up an ArcSight Web server for v5.0 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.)



- 23 Select whether you want to install the Manager as a service. The option you select from these Manager startup options will take effect when the Manager machine reboots.
- 24 On Unix platforms, if you get a message saying changes to the service configuration require root privileges, follow the steps listed in the message.
- 25 During the upgrade, the v5.0 GA `config/server/agentURLMapping.csv` file is saved with the file extension `.previous` in the `config/server` directory of v5.0 SP1 `ARCSIGHT_HOME`. If you customized this file in v5.0 GA and want to use it for v5.0 SP1, rename the saved file to remove the `.previous` extension. That is, rename `agentURLMapping.csv.previous` to `agentURLMapping.csv`.
- 26 On successful completion of the upgrade, you will see a message to that effect.
- 27 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 v5.0 GA to the v5.0 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`.

On Unix machines, make sure you have the Firefox web browser installed and available to view the summary report.

- 28 Click **Done** in the last screen to exit the wizard.

You have upgraded ArcSight Manager to v5.0 SP1.

## Post-Upgrade Tasks

You are required to do the following after upgrading your Manager to v5.0 SP1:

- Validate your resources after you have upgraded your Manager especially if you have assets in system zones. To do so, run the following from the Manager's `\bin` directory:

```
arcsight resvalidate -persist
```

You need to have the same `ARCSIGHT_JVM_OPTIONS` as your v5.0 GA Manager when running this. See [Step d on page 15](#) for details on setting `ARCSIGHT_JVM_OPTIONS`.

- You are required to manually run the following script to disable the oracle nightly statistics that run over arcsight schema. Run the following commands while logged in as the oracle user (`su -oracle`):

```
% arcdbutil sql

Enter user-name: / as sysdba

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

- Run the following script from the Manager's `/bin` directory to check your resource references:

```
arcsight refcheck -f true
```

This command will fix any broken resource references and also persist those changes.

- File resources are not handled properly during ESM upgrade. This results in unassigned file resources after the upgrade. For example, the `.art` files are created as new file resources in ESM v5.0 GA and get new version IDs during the upgrade. The original files are stored in the Files resource under the Unassigned folder. To work around this issue, you can remove the unassigned `.art` files after an upgrade because they are duplicates. These `.art` files can be safely deleted.

If you are upgrading from v4.5 SP3 Patch 1 to v5.0 Patch 1, on Linux, and in a French locale, use the following procedure for starting the Manager:

- 1 Find and open the file `.bash_profile` in the `<USER_HOME>` folder.
- 2 Add the following two lines to this file:

```
LANG=fr_FR.UTF-8
export LANG
```

- 3 You can now start the Manager.

Before you upgrade from v5.0 Patch 1 to v5.0 SP1, remove the two added lines from that file.



The Manager will be updating search index in the initial few minutes after it starts. So, you may see a performance impact while the search index is being updated.

---

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

## Upgrading the Index

The steps in this section are needed **only** if you plan to use the Domain Field Sets feature and your license key has enabled this feature. If you do not plan to use the Domain Field Sets feature, then upgrading the index is not required.

These steps can be performed either now or at any time in the future. Decide whether you want to upgrade the indexes now or later, based on the following two factors:

- Amount of available space in the `ARC_EVENT_INDEX` tablespace  
The `dbcheck` script provides you both, the amount of space available and the amount of space required for index upgrade. If the amount of space required for index upgrade is lesser than the available space, you can add additional disk space.

- Length of system downtime allocated for this upgrade

Because upgrading an index depends on the size of the event table, the Retention Period, and other aspects of the database configuration, it may require several hours to complete. Check the output of `dbcheck` to determine the estimated time it will take to complete the index upgrade.

After the upgrade to v5.0 SP1 Manager is complete, run the following command in `ARCSIGHT_HOME/bin` to start the Index Upgrade wizard. (Be sure to avoid running this from `MANAGER_ARCSIGHT_HOME`, or it will not connect to the database.)

```
arcsight upgrade index
```

The Index Upgrade wizard prompts you for database information such as database host name, port name, instance name, user name and password, and admin user name and password. Step through the wizard screens and enter the information it requests. Start the Manager after the wizard completes.

## 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
```



**Note**

`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          | Red Hat Enterprise Linux 4.0 (RHEL 4) WS 32-bit Update 8 | x86-compatible multi-CPU system with 2-4 GB RAM           |
|                | Red Hat Enterprise Linux 4.0 (RHEL 4) AS 64-bit Update 8 |   |
|                | Red Hat Enterprise Linux (RHEL 5.4) Desktop 32-bit       |   |
| Solaris        | Sun Solaris 10 (10/09) SPARC, 64-bit                     | Sparc-compatible multi-CPU system with 2-4 GB RAM         |
| Windows        | Microsoft Windows Server 2003 R2 (SP2) 32-bit            | x86-compatible single or multi-CPU system with 1-2 GB RAM |
|                | Microsoft Windows Server 2003 R2 (SP2) 64-bit            |   |
|                | Microsoft Windows Server 2008 SP2 64-bit                 |   |
|                | Microsoft Windows Vista SP2 64-bit                       |   |
|                | Microsoft Windows Vista SP2 32-bit                       |   |
|                | Microsoft Windows XP Professional SP3 32-bit             |   |
| Macintosh OS X | Macintosh OS X 10.5.6 64-bit                             |   |



Refer to the ArcSight ESM Product Lifecycle document available on the ArcSight Customer Support web site 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 v5.0 SP1 Console installation file to a different machine, transfer it to your Console machine.
- 3 Run the installation file appropriate for your platform:
  - ◆ **On Windows:**  
Double-click `ArcSight-5.0.1.xxxx.0-Console-Win.exe`
  - ◆ **On Solaris:**  
Run the following command.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-Solaris.bin
```

  
To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-Solaris.bin -i console
```
  - ◆ **On Macintosh:**  
Run the following command.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-MacOSX.bin
```

  
To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-MacOSX.bin -i console
```
  - ◆ **On Linux:**  
Run the following command.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-Linux.bin
```

  
To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.  
  

```
./ArcSight-5.0.1.xxxx.0-Console-Linux.bin -i console
```

  
The installer launches the Installation Process Check window.
- 4 Click **Next** in the Installation Process Check window.
- 5 Step through the Installation wizard screens. Specifically, enter values as described below for the following wizard screens:
  - ◆ **Introduction**—Read the Introduction and click **Next**.
  - ◆ **License Agreement**—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**.
  - ◆ **Special Notice**—Read the notice and click **Next**.

- ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v5.0 SP1 that is different from where the existing Console is installed.



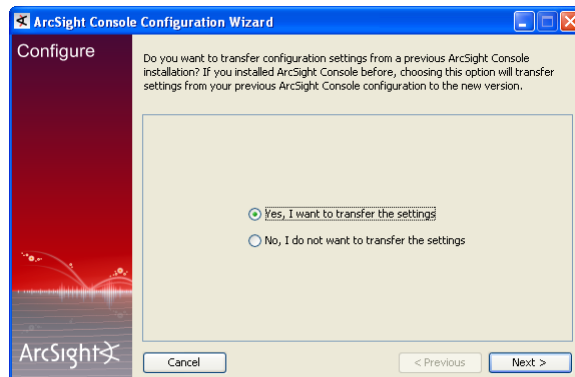
Do NOT install v5.0 SP1 Console in the same location as the existing Console.

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) or **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. Click **Next**.
- ◆ **Pre-Installation Summary**—Review the settings and click **Install**.

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

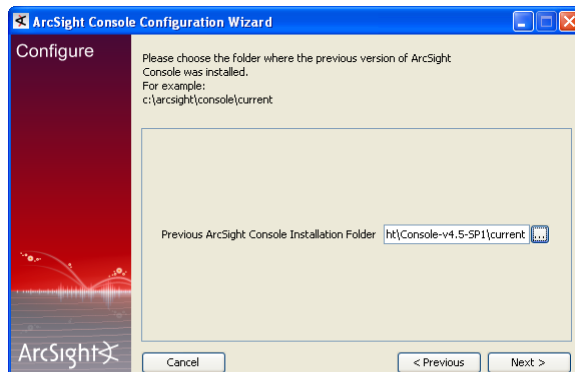
- The Console installation program detects a previous installation and provides you an option to copy your existing settings to the new Console. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type. Select **Yes, I want to transfer the settings** and click **Next**.



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

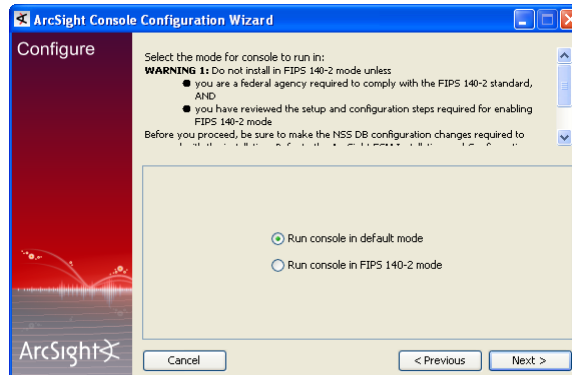


Be sure to select `<ARCSIGHT_HOME>\current` directory of your previous installation as shown in the screen image below.



Click **Next**.

- 8 (Applicable when upgrading in default mode only)** In the following screen, select **Run console in default mode** and click **Next**:



- 9** See the *ArcSight ESM Installation and Configuration Guide* for details on the remaining screens for installing a Console using the installation wizard.

If you are upgrading from v4.5 SP3 Patch 1 to v5.0 Patch 1, on Linux, and in a French locale, use the following procedure:

- a** Find and open the file `.bash_profile` in the `<USER_HOME>` folder.
- b** Add the following two lines to this file:

```
LANG=fr_FR.UTF-8
export LANG
```

Before you upgrade from v5.0 Patch 1 to v5.0 SP1, remove the two added lines from that file.

- 10** Start the ArcSight Console.

A What's new Quick Start screen is displayed automatically. This screen summarizes the new features in ESM v5.0 SP1.

- 11** After you have upgraded a Console to v5.0 SP1:

- 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.

- 12** 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.

# Upgrading ArcSight Web

## Upgrading ArcSight Web



The list of supported platforms for ArcSight Web v5.0 SP1 is same as the one for ArcSight Manager v5.0 SP1.

Note

The following web browsers are supported in this release:

| Platform       | Supported Browsers                          |
|----------------|---|
| Solaris SPARC  | Firefox 2.0, 3.0                            |
| Windows        | Internet Explorer 7.0, 8.0 Firefox 3.0, 3.6 |
| Linux          | Firefox 3.0, 3.6                            |
| Macintosh OS X | Safari 2.0, 3.1, Firefox 3.0, 3.6           |

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 v5.0 SP1 ArcSight Web installation file to a different machine, transfer it to your ArcSight Web machine.
- 4 Run the installation file appropriate for your platform:

◆ **On Windows:**

Double-click `ArcSight-5.0.1.xxxx.0-Web-Win.exe`

◆ **On Solaris:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Web-Solaris.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Web-Solaris.bin -i console
```

◆ **On AIX:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Web-AIX.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Web-AIX.bin -i console
```

◆ **On Linux:**

Run the following command.

```
./ArcSight-5.0.1.xxxx.0-Web-Linux.bin
```

To install in console mode, run the following command from the shell prompt and then follow the instructions in the window.

```
./ArcSight-5.0.1.xxxx.0-Web-Linux.bin -i console
```

The installer launches the Introduction window.

**5** Click **Next** in the Installation Process Checklist window and the Introduction window.

**6** Step through the Installation Wizard screens. Specifically, enter values as described below for the following Wizard screens:

- ◆ **License Agreement**—The “I accept the terms of the License Agreement” radio button is 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**.
- ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v5.0 SP1 that is different from where the existing Web is installed.



**Note**

Do NOT install v5.0 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.

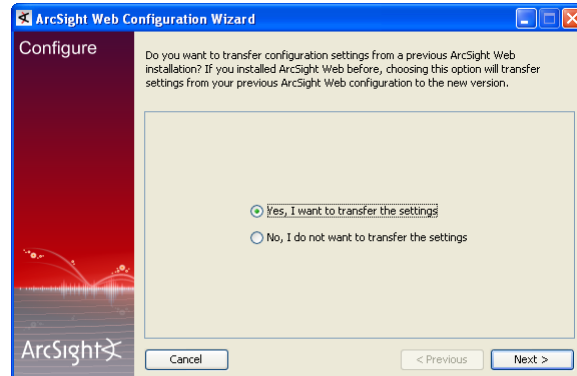
---

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

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

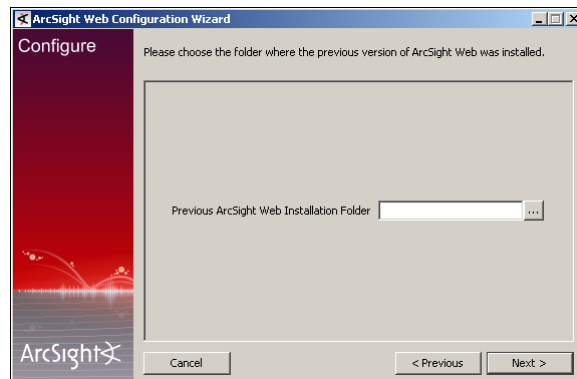
**7** The Web installation program detects a previous installation and provides you an option to copy your existing settings to the new Web. Settings such as connection

information including the Manager host name and port number, and authentication information including authentication type.



Click **Next**.

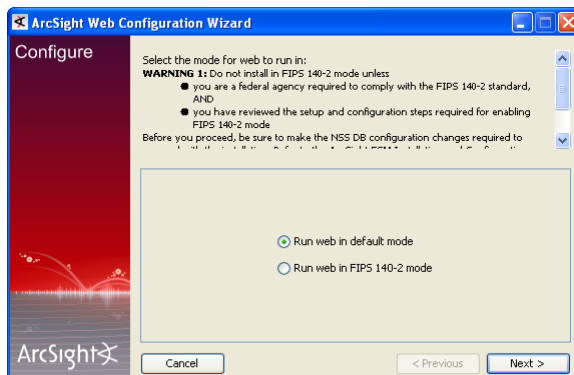
- 8** If you selected **Yes, I want to transfer the settings**, the Web installation program prompts you to enter the location for your previous installation.



Navigate or enter the location for the previous ArcSight Web installation and click **Next**.

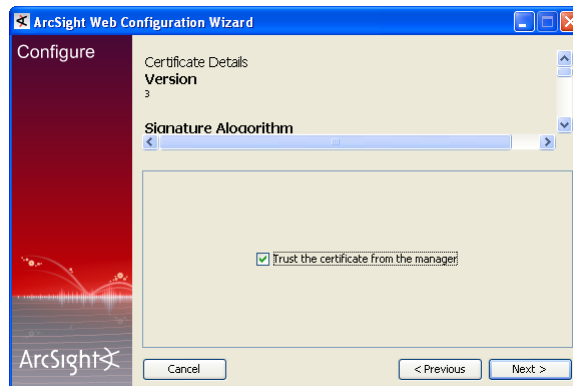
If you selected **No, I do not want to transfer the settings** option, you will be prompted to select the mode in which you are upgrading after you click **Next**.

- 9 (Applicable when upgrading in default mode only)** In the following screen, make sure that you select **Run web in default mode** option and click **Next**:



- 10** Follow the prompts in the next few screens.

- 11** Make sure to check the box in the following screen in order to trust the Manager's certificate.



- 12** Continue with the upgrade by following the instructions on the screens.

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

If you are upgrading from v4.5 SP3 Patch 1 to v5.0 Patch 1, on Linux, and in a French locale, use the following procedure:

- a** Find and open the file `.bash_profile` in the `<USER_HOME>` folder.
- b** Add the following two lines to this file:  

```
LANG=fr_FR.UTF-8
export LANG
```
- c** Before you upgrade from v5.0 Patch 1 to v5.0 SP1, remove the two added lines from that file.

- 13** Start ArcSight Web.



# 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 v5.0 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 v5.0 GA or v5.0 Patch 1 *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**).
- For existing assets, if two assets **in the same zone** have the same host name or IP address one of them becomes invalid after the ESM upgrade to v5.0 SP1. This may happen for assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In v5.0, only the host name is extracted from the FQDN and used when comparing the two assets.

For example, if two assets have FQDNs "myhost.mycompany.com" and "myhost.mycompany.us.com", only the value "myhost" is used to compare them and their domain names are ignored. Since the host name is identical, these two assets are considered as conflicting assets and one of them becomes invalid.

If you would like to override this and use the FQDN instead, set the following property in the `server.properties` file:

```
asset.lookup.hostname.resolve.without.domain=true
```

- **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 v5.0 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 v5.0 GA or v5.0 Patch 1 zones.
  - ◆ Delete any invalid zones that you no longer want to keep.
  - ◆ If you made customizations to the standard v4.5 SP1/SP2/SP3 zones, manually edit the new resource to restore the customizations you made to the v5.0 GA 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.
- If you have upgraded your ESM installation more than once (for example, from v4.0 to v4.5, then v5.0 GA and are now upgrading to v5.0 SP1), you might see resources that do not show as deprecated in the [/All \[resource\\_types\]/Deprecated/](#) group. To check whether a resource is deprecated or not, you have to open the resource and see if the "Deprecated" checkbox is checked. If you see a non-deprecated resource in one of their [/All \[resource\\_types\]/Deprecated/](#) groups, you can remove the resource from that group (that resource is likely just linked into that group, so you can remove the link).
- **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 v5.0 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.

# Upgrading ArcSight SmartConnectors

---

At a minimum, the SmartConnectors must be running version 3.1.0.4021.0. 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 version 4.0.1.4785.0 or above in order to avoid DST-related issues. Refer to the DST documents provided on the ArcSight Support download site for details.

Download installation files as appropriate for your SmartConnector platforms. To leverage the ESM v5.0 schema, you will need to use SmartConnector version 4.8.1 at a minimum. Use the [.aup](#) file for remote upgrade.

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.



## Chapter 8

# Upgrading Oracle Database to 11g

---

You can upgrade your Oracle Database after you have finished upgrading all the ESM components to v5.0 SP1 and verified that they have upgraded successfully. Before you begin, stop the Oracle database and take a cold backup of the entire database.



Caution

This is an important precaution that will ensure that you have the option to fallback to the previous version should something go awry during the upgrade.



Note

**For Windows platform only:** Before you upgrade your Oracle instance from version 10g to 11g, make sure to delete the `<ORACLE_HOME>` environment variable if it was previously set and reboot your database server.

**For Red Hat Linux Enterprise Edition 4:** Oracle 11g is not supported.

## Required Oracle Packages

**Before** you install or upgrade to Oracle 11g verify that you have the following required packages for Oracle 11g installed on your database machine.

### On 32-bit Linux:

The following packages (or later versions) must be installed:

#### On Red Hat Enterprise Linux 5

```
binutils-2.17.50.0.6
compat-libstdc++-33-3.2.3
compat-libstdc++-33-3.2.3 (32 bit)
elfutils-libelf-0.125
elfutils-libelf-devel-0.125
gcc-4.1.2
gcc-c++-4.1.2
glibc-2.5-24
glibc-2.5-24 (32 bit)
glibc-common-2.5
glibc-devel-2.5
glibc-devel-2.5 (32 bit)
glibc-headers-2.5
ksh-20060214
libaio-0.3.106
libaio-0.3.106 (32 bit)
libaio-devel-0.3.106
libaio-devel-0.3.106 (32 bit)
```

```
libgcc-4.1.2
libgcc-4.1.2 (32 bit)
libstdc++-4.1.2
libstdc++-4.1.2 (32 bit)
libstdc++-devel 4.1.2
make-3.81
numactl-devel-0.9.8.x86_64
sysstat-7.0.2
UnixODBC-2.2.11 (32 bit) or later
UnixODBC-devel_2.2.11 (64 bit) or later
```

## On 64-bit Linux:

The following packages (or later versions) must be installed:

### On Red Hat Enterprise Linux 5

```
binutils-2.17.50.0.6
compat-libstdc++-33-3.2.3
gcc-4.1.2
glibc-2.5-24
glibc-common-2.5
glibc-devel-2.5
libaio-0.3.106
libaio-devel-0.3.106
libstdc++-4.1.2
libstdc++-devel 4.1.2
make-3.81
sysstat-7.0.2
unixODBC-2.2.11 (32 bit) or later
unixODBC-devel-2.2.11 (64 bit) or later
unixODBC-2.2.11 (64 bit ) or later
```

## Upgrading Oracle

To upgrade from Oracle 10g to 11g, you must first install Oracle 11g software and then upgrade the 10g instance to 11g.



**Caution**

Before upgrading your Oracle to 11g:

- 1 Shut down all the external oracle sessions that are connected to the oracle instance. This is required in order to upgrade the instance to Oracle 11g.
- 2 Shut down the TNS listener.
- 3 **If you had installed Oracle Enterprise Manager** with your Oracle 10g installation, you must shut it down before you start the upgrade. To shut down the Oracle Enterprise Manager run the following command from the ArcSight Database's bin directory:

```
emctl stop dbconsole
```

---

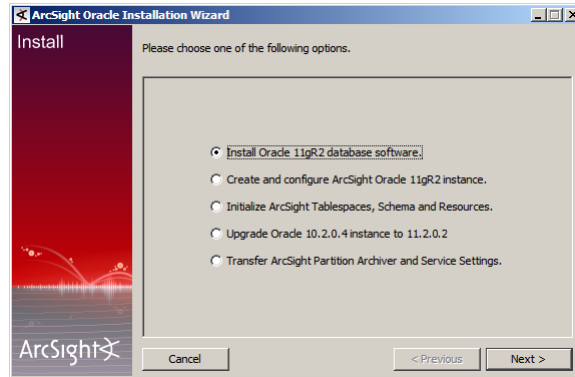
### Upgrading Oracle 10g Software to 11g

You will be required to upgrade your Oracle software to 11g before you upgrade the Oracle instance. To do so:

- 1 Run the following command from the bin directory of your ArcSight Database installation:

```
./arcsight databasesetup
```

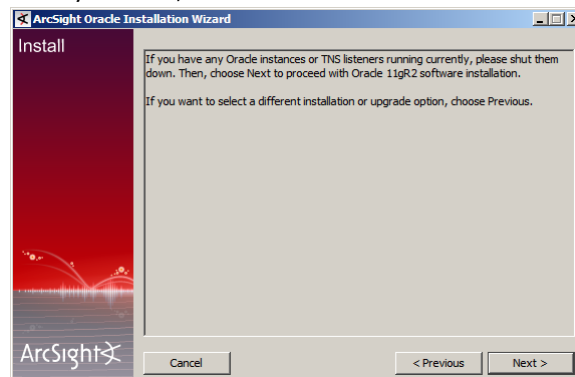
- 2 Select **Install Oracle 11gR2 database software** and click **Next**.xx



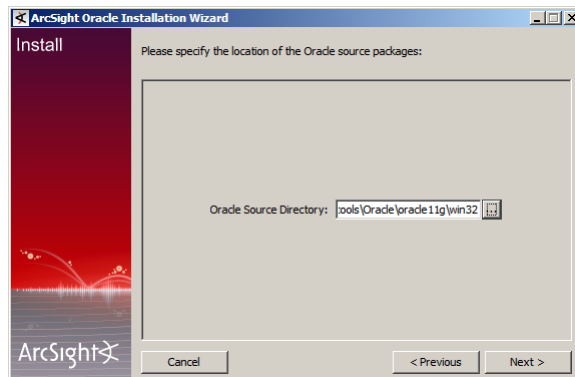
**Note**

The screen shots in this guide that show 11.2.0.2, will show 11.2.0.1 when you are installing Windows.

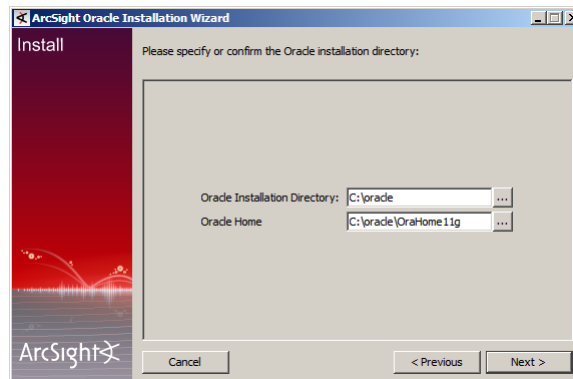
- 3 Shut down the TNS listener or any Oracle instances that are running, if you have not already done so, and click **Next**.



- 4 Navigate to the location of the Oracle source packages and click **Next**.

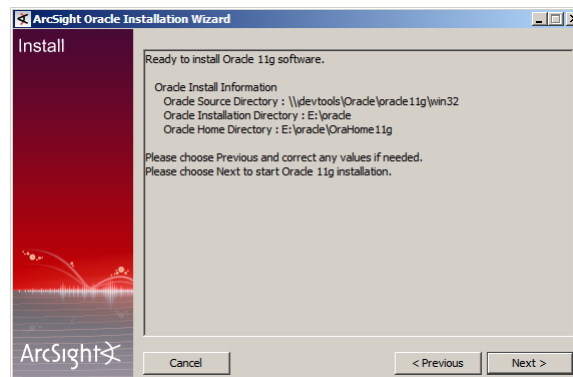


- 5 Enter the file path for Oracle 11g, as shown in the example in the screen image below, then click **Next**.

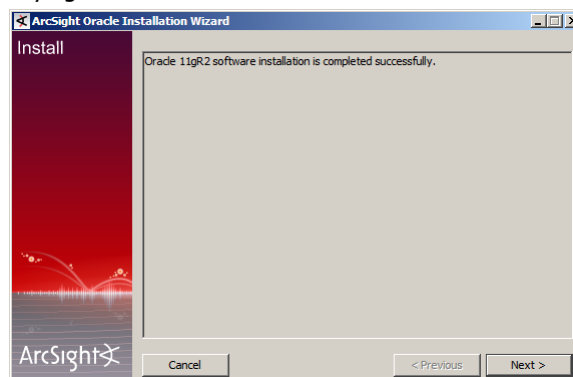
**Caution**

- Verify that the Oracle installation directory path and the Oracle Home path do not contain any spaces.
- If you are upgrading from Oracle 10g, and Oracle Home shows the path to the Oracle 10g installation, *be sure* to change it. If you do not change it, you install 11g over 10g and you cannot revert to the previous installation if something goes wrong.

- 6 Review the pre-installation information and if satisfied, click **Next**.



- 7 After the Oracle 11g software has been installed successfully, you will see a message saying so. Click **Next**.



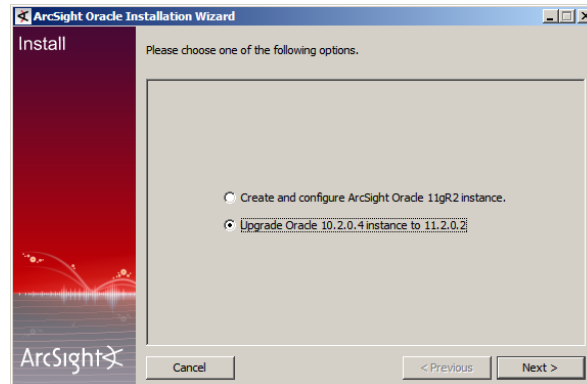
Now, you can either create a new Oracle 11g instance or upgrade your existing 10g instance to 11g.



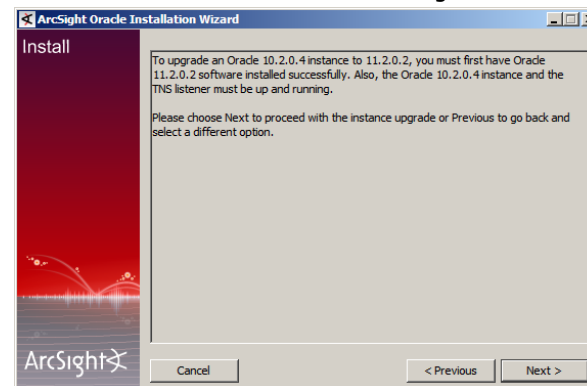
## Upgrading a 10g Oracle Instance to 11g

To upgrade your Oracle 10g instance:

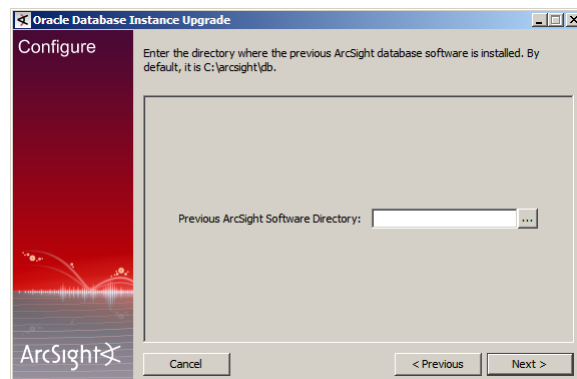
- 8 Select **Upgrade Oracle 10.2.0.4 instance to 11.2.0.2** (11.2.0.1 on Windows) and click **Next**.



- 9 Start the TNS listener and the Oracle 10g instance and then click **Next** in this screen.

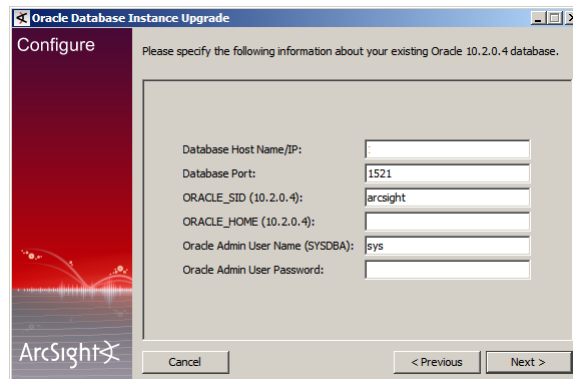


- 10 Enter the location where your current ArcSight Database (v5.0 GA) exists and click **Next**.



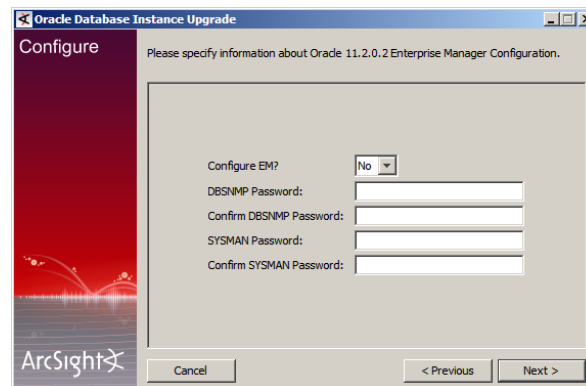
The installation wizard uses this information to retrieve the database host name and port.

- 11** Enter the information about the previously-existing Oracle 10g software and click **Next**.



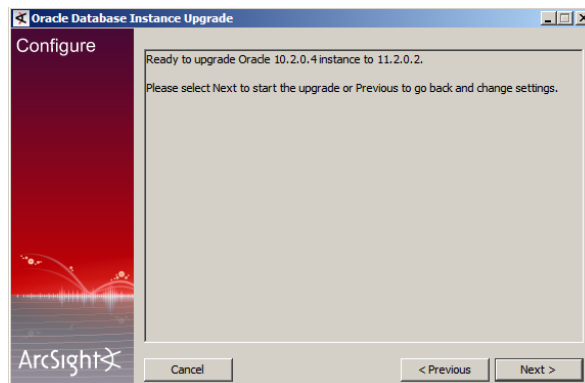
The screenshot shows the 'Configure' window of the 'Oracle Database Instance Upgrade' wizard. The title bar reads 'Oracle Database Instance Upgrade'. The window has a red sidebar on the left with the 'ArcSight' logo. The main area has a light gray background with the text 'Please specify the following information about your existing Oracle 10.2.0.4 database.' Below this text are six input fields: 'Database Host Name/IP:', 'Database Port:' (containing '1521'), 'ORACLE\_SID (10.2.0.4):' (containing 'arcsight'), 'ORACLE\_HOME (10.2.0.4):', 'Oracle Admin User Name (SYSDBA):' (containing 'sys'), and 'Oracle Admin User Password:'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 12** Select whether you want to configure the Enterprise Manager and enter the information for DBSNMP and SYSMAN and click **Next**.



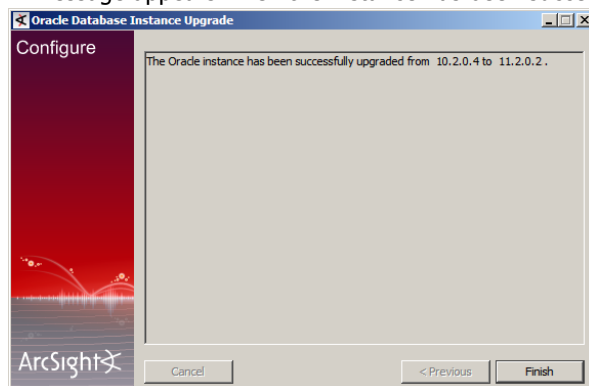
The screenshot shows the 'Configure' window of the 'Oracle Database Instance Upgrade' wizard. The title bar reads 'Oracle Database Instance Upgrade'. The window has a red sidebar on the left with the 'ArcSight' logo. The main area has a light gray background with the text 'Please specify information about Oracle 11.2.0.2 Enterprise Manager Configuration.' Below this text are five input fields: 'Configure EM?' (a dropdown menu set to 'No'), 'DBSNMP Password:', 'Confirm DBSNMP Password:', 'SYSMAN Password:', and 'Confirm SYSMAN Password:'. At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 13** The next screen will inform you that the instance upgrade is about to begin. Click **Next**.



The screenshot shows the 'Ready to upgrade' window of the 'Oracle Database Instance Upgrade' wizard. The title bar reads 'Oracle Database Instance Upgrade'. The window has a red sidebar on the left with the 'ArcSight' logo. The main area has a light gray background with the text 'Ready to upgrade Oracle 10.2.0.4 instance to 11.2.0.2.' and 'Please select Next to start the upgrade or Previous to go back and change settings.' At the bottom are three buttons: 'Cancel', '< Previous', and 'Next >'.

- 14** A message appears when the instance has been successfully upgraded. Click **Finish**.



You have upgraded your Oracle database and the instance to 11g.



# Index

---

## A

- ArcSight Database
  - preparing to install 5
  - supported platforms 5

## C

- cold backup 41

## D

- database components 5
- database system tables 14
- downloading
  - Console files 3
  - Database files 2
  - Manager files 3
  - SmartConnector files 2
  - Web files 3
- downloading files 2

## E

- excluding
  - resources to validate 24

## F

- FIPS 1

## H

- heap size 15
- hierarchical manager
  - upgrade 2

## I

- Index, upgrading 26
- invalid resources 38
- IO transfer speed 9

## L

- locale issues 18, 32, 36

## M

- Manager 13

## O

- Oracle packages 41

## P

- Partition Archiver service 7
- platforms, supported for Manager 13

## R

- redundant name check 20
- Related documentation 3
- resource validation 23

## S

- SmartConnectors 39
- system content length 19
- system resources, backup 14

## U

- updating
  - Partition Archiver service 27
- upgrade
  - hierarchical manager 2
  - preparing for 1
  - steps 1
- upgrading
  - steps to check your database 6

