



HP ArcSight ESM

Software Version : ESM 5.5 to ESM 5.6

Upgrade Guide

August 19, 2015



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

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

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

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

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

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

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

This document is confidential.

Contact Information

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

Revision History

Date	Product Version	Description
08/18/2015	5.6	Updated for ESM 5.6 release.

Contents

Chapter 1: Preparing for the Upgrade	5
Upgrade Support	5
Oracle Upgrade Support	5
Summary	5
Downloading Installation Files, Scripts, and Other Documents	6
Preparing Existing Content for Upgrade	7
Chapter 2: Upgrading ArcSight Database Components	9
Upgrading the Oracle Software	9
Preparing the ArcSight Database Components	9
Upgrading the ArcSight Database Software and Partition Archiver	11
Transferring Partition Archiver Settings	14
Chapter 3: Upgrading Oracle Database	17
Required Oracle Packages on x86 64-bit Linux	17
Before Upgrading to Oracle 11.2.0.4	18
Upgrading Oracle	20
Upgrading the Oracle Software from 11.2.0.3 to 11.2.0.4	20
Upgrading the 11.2.0.3 Oracle Instance to 11.2.0.4	23
Chapter 4: Upgrading ArcSight Manager	27
Preparing for the Manager Upgrade	27
Upgrading the ArcSight Manager	28
Post-Upgrade Tasks	37
Upgrading the Index	37
Updating and Starting the Partition Archiver Service	38
Chapter 5: Upgrading ArcSight Console	41
Chapter 6: Upgrading ArcSight Web	45
Chapter 7: Checking the State of Existing Content after the Upgrade	49
Chapter 8: Upgrading ArcSight SmartConnectors	53
Upgrading the Forwarding Connector	53

Chapter 9: Upgrading Hierarchical or Other Multi-Manager ESM Installations to 5.6 55

 Summary 55

 Upgrading a Hierarchical Deployment 55

 Upgrading a High Availability (Failover) Configuration 56

 Upgrading a Peer-to-Peer Configuration 56

Index 57

Chapter 1

Preparing for the Upgrade

This chapter describes the steps required to upgrade the ArcSight ESM components to 5.6.

Upgrade Support

ESM 5.6 is only supported on 64-bit Windows and Linux. The upgrade path for this release is ESM 5.5 (with the latest patch) to ESM 5.6.

Upgrade ESM in the same mode (FIPS or default) as the current installation. Upgrading from an existing FIPS mode installation to default mode or vice versa is not supported.



ArcSight ESM supports the Federal Information Processing Standard (FIPS), as an alternative to running ESM in **default mode** (non-FIPS). FIPS is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive but Unclassified (SBU) information should meet these standards.

Oracle Upgrade Support

ESM 5.6 uses Oracle 11.2.0.4. If you are using Oracle 11.2.0.3, you can upgrade to Oracle 11.2.0.4 after upgrading the ArcSight Database component. See [Chapter 3, Upgrading Oracle Database, on page 17](#) for details on how to upgrade Oracle.

Summary

After the preparations included in this chapter, upgrading ArcSight ESM involves the following steps:

- ["Upgrading ArcSight Database Components" on page 9](#)
- ["Upgrading Oracle Database" on page 17](#)
- ["Upgrading ArcSight Manager" on page 27](#)
- ["Upgrading ArcSight Console" on page 41](#)
- ["Upgrading ArcSight Web" on page 45](#)
- ["Checking the State of Existing Content after the Upgrade" on page 49](#)
- ["Upgrading ArcSight SmartConnectors" on page 53](#)

If you have a hierarchical or a multi-ArcSight Manager setup, also see [Chapter 9, Upgrading Hierarchical or Other Multi-Manager ESM Installations to 5.6](#), on page 55.

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 to 5.6. Unless noted, all files are available at the HP support website.

You can download files to one of the following destinations:

- 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 files for all components as listed below directly to the component machines where they will be installed.



Note

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

Visit the following site for information and instructions:

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

For the SmartConnector:

Download installation files as appropriate for your SmartConnector platforms. To leverage the ESM 5.6 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 the Console, click **Help | About**. The current version is displayed in `5.5.0.xxxx.n` format for 5.5, 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-5.6.0.xxxx.0-DB-Win.exe`
 - ◆ `ArcSight-5.6.0.xxxx.0-DB-Linux.bin`

For the Manager:

- 1 Check the current ArcSight ESM version you are running on the Manager. To check the version, in a Console that connects to the Manager, click **Help | About**. The current version is displayed in `5.5.0.xxxx.n` format for 5.5, where `xxxx` is the build number and `n` is the patch number.
- 2 Download the compressed file containing the Manager installation file as appropriate for your platform. These installation files are available:
 - ◆ `ArcSight-5.6.0.xxxx.0-Manager-Win64.zip`
 - ◆ `ArcSight-5.6.0.xxxx.0-Manager-Linux64.zip`

For the Consoles:

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

- ArcSight-5.6.0.xxxx.0-Console-Win.exe
- ArcSight-5.6.0.xxxx.0-Console-Linux.bin

For ArcSight Web:

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

- ArcSight-5.6.0.xxxx.0-Web-Win.zip
- ArcSight-5.6.0.xxxx.0-Web-Linux.zip

Other Documentation:

In addition to this Upgrade Guide, refer to the following 5.6 documents to complete the upgrade process:

- ArcSight ESM 5.6 Release Notes
- ArcSight ESM Installation and Configuration Guide
- ArcSight ESM Administrator's Guide
- ArcSight ESM System Content Reference Guide

These documents are available for download from HP at <https://softwaresupport.hp.com/>.



On Linux, make sure that you have a Firefox web browser installed and available in your 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 set up Firefox, you will see a "java.io.IOException: firefox: not found" exception at the end of managerwizard.log. You can manually open the upgrade summary report from "`<path_of_manager>/upgrade/out/<timestamp>/summary.html`" using any available browser on your system.

On Windows, Internet Explorer is the default browser. IE displays the report after the upgrade. You are not required to open it manually.

Preparing Existing Content for Upgrade

Every content situation is a unique blend of ArcSight-supplied resources in various states, and customer-supplied resources: those created from scratch, and those created by copying and modifying an existing ArcSight resource. When preparing existing content for upgrade, consider the following:

- **Back up existing resources.** Always back up all resources before upgrading. You can do this using the Packages import/export facility described in the ArcSight Console User's Guide topic "Managing Resources > Managing Packages." In some cases, modifications you have made to existing ArcSight resources may require manual reconfiguration after the upgrade. You can use the backup copy as a reference during reconfiguration.
- **Assets Resource.** The Assets resource is part of the ESM asset model, which identifies and maps the network devices participating in the event flow. During the upgrade, existing assets upgrade seamlessly.

If an asset is disabled after the upgrade, restore it manually by fixing its IP address range to match a valid zone.

- **Zones Resource.** ESM uses zones to identify the network devices that contribute to the event stream by their IP addresses.
 - ◆ If you customized standard ESM zones directly (with the original resource ID), the upgrade will overwrite your customizations. Be sure to back up your customizations so you can restore them manually after the upgrade.
 - ◆ If you created your own zones, any that overlap standard ESM zones are disabled and placed in the Disabled Zones group.
 - ◆ Before the upgrade, manually note what zones you have and their locations. Manually verify the location and status of these zones after the upgrade.

Chapter 2

Upgrading ArcSight Database Components

This chapter is about preparing the ArcSight Database components for version 5.6.

The following topics are covered here:

["Upgrading the Oracle Software" on page 9](#)

["Preparing the ArcSight Database Components" on page 9](#)

["Upgrading the ArcSight Database Software and Partition Archiver" on page 11](#)

Upgrading the Oracle Software

ESM 5.6 uses Oracle 11.2.0.4. If you are using Oracle 11.2.0.3, you can upgrade to Oracle 11.2.0.4 after upgrading the ArcSight Database component. See [Chapter 3, Upgrading Oracle Database, on page 17](#) for details on how to upgrade Oracle.

If you are using Oracle 11.2.0.2 on Windows, you must first upgrade your Oracle software to 11.2.0.3 by upgrading to ESM 5.5 (with the latest patch) before upgrading to 5.6. Refer to the release notes for the target ESM version (ESM 5.5 with the latest patch) for detailed instructions on upgrading to it.

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 are supported. Refer to the *HP ArcSight ESM Support Matrix* document available on <https://protect724.hp.com> 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 the Release Notes that you downloaded with the patch.
- 3 Set Shell Limits for the oracle User:
 - a Add or edit the following lines in the `/etc/security/limits.conf` file, if they do not already exist:

```
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft nofile 1024
```

```
oracle hard nofile 65536
oracle soft stack 10240
```

- b** Add or edit the following line in the `/etc/pam.d/login` file, if it does not already exist:

```
session required pam_limits.so
```

- 4 On Windows**, when upgrading from Oracle 11.2.0.3 to 11.2.0.4, if Oracle 11.2.0.3 is installed on any drive other than the C: drive, it can cause access denied errors. Follow this procedure before you start the installation:

- a** Shutdown the Oracle Services. (This is a specific exception to the warning against doing this in Upgrade section.)
- b** Set the global environment variable `ORACLE_HOME` to the directory where Oracle is installed on your system. (This causes the installer to create a `.backup` directory.)
- c** Reboot the system.

- 5** Perform these steps to identify if your 5.5 (with the latest patch) database is ready for upgrade:

- a** Shut down your currently installed 5.5 (with the latest patch) ArcSight Web, ArcSight Manager, and Partition Archiver.



If you had partition archiving enabled and would like to disable the archiving now, check the Console for any partitions that have a reactivated status. If you see partitions with a reactivated status, deactivate those partitions before disabling the Partition Archiver.

For instructions about shutting down your ArcSight Manager, see the ArcSight ESM Administrator's Guide.

- b** In `<ARCSIGHT_HOME>/bin` of your 5.5 (with the latest patch) database installation, run the following command:

On Windows:

```
arcsight dbcheck
```

On Linux:

```
./arcsight dbcheck
```

The following log files are listed in the Database's `<ARCSIGHT_HOME>/logs/dbcheck` directory:

- DatabaseInfo.htm
- EventIndexInfo.htm
- TablespaceInfo.htm
- MiscInfo.log
- OraclePatchInventory.log
- TableStatsInfo.htm
- PartitionInfoV40.htm
- PartitionStatsInfo.htm
- ResourceCountV40.htm

- `index.htm`

To view a log file, open the `index.htm` file and click the appropriate link.

If the log files contain errors or warnings, resolve issues that might be causing those errors. HP strongly recommends resolving all issues before proceeding with the upgrade. If you need assistance, contact Customer Support on the HP SSO website and be prepared to send the `dbchecklogs.tar.gz` or `dbchecklogs.zip` file (as appropriate for your platform) if requested.

- 6 Archived partitions with archive type **uncompressed** should not be in reactivated state during the Manager upgrade. Deactivate such partitions before you upgrade Manager.



This is only valid for archive type **uncompressed**.

Note

Upgrading the ArcSight Database Software and Partition Archiver

- 1 If you downloaded the ArcSight Database 5.6 installation file on a different machine, transfer it to your database machine.
- 2 If you have Partition Archiver service running on your database machine, shut it down.
- 3 Log in as **root** on Linux and **Administrator** on Windows on the database server.
- 4 Run the database installation executable appropriate for your platform:

◆ **On Windows:**

Double-click `ArcSight-5.6.0.xxxx.0-DB-Win.exe`

◆ **On Linux:**

Run the following command.

```
./ArcSight-5.6.0.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-5.6.0.xxxx.0-DB-Linux.bin -i console
```

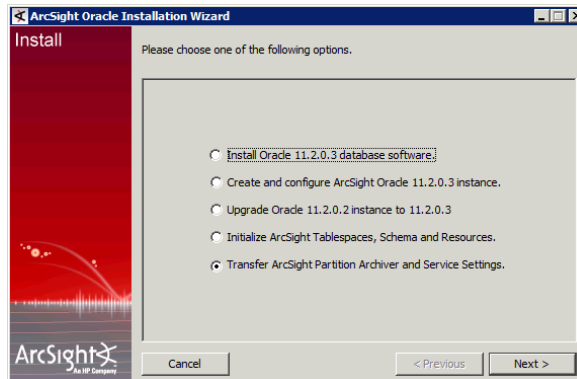
The installer launches the Introduction window.

- 5 Click **Next** in the Introduction screen.
- 6 In the License Agreement screen, read the agreement text, click **I accept the terms of the License Agreement** radio button, and click **Next**.

This radio button is disabled until you scroll to the bottom of the agreement to help ensure that you have read the agreement.

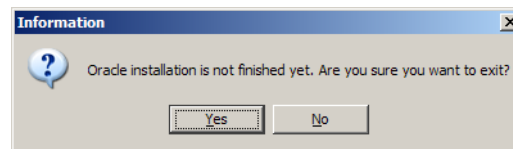
- 7 Read the Special Notice and click **Next**.
- 8 Enter the location where you want to install the 5.6 database software. Choose a location that is different from where you have the 5.5 (with the latest patch) database software installed. Click **Next**.
- 9 Review the pre-installation summary and click **Install**.

- 10 Review the options on the following screen. Select an option that suits your needs; however, if you are installing Oracle, make sure to stop Oracle services and the TNS Listener. Then click **Next**.



- ◆ Click **Cancel** if:
 - you do not want to upgrade your Oracle installation and/or
 - you did not have Partition Archiver configured in 5.5 (with the latest patch)

Click **Yes** in the following message box:



Click **Done** in the last wizard screen. You have finished upgrading the ArcSight Database software.



On Linux 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 5.5 (with the latest patch), transfer the Partition Archiver settings to your ArcSight Database 5.6 in addition to upgrading it. So, select **Transfer ArcSight Partition Archiver and Service Settings** and click **Next**. See [“Transferring Partition Archiver Settings” on page 14](#) for details on the wizard screens that follow.



Notes about database upgrade and archives

- The Partition Archiver service does not start automatically. Therefore, you must start the service manually, but wait until you have upgraded Manager to 5.6. See the section, [“Updating and Starting the Partition Archiver Service” on page 38 in Chapter 4, Upgrading ArcSight Manager, on page 27](#).
- If you have archived partitions and you had set up your Partition Archiver to archive with type uncompressed, back up your archive folder (that contains the partition that you are trying to reactivate) before reactivation.

Keep in mind that when you reactivate the partition, it succeeds 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 helps 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
```



Run this script every time you make storage hardware changes that affect IO transfer speeds.

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

If you want to avoid the problem of expired passwords, then do the following to set the password to never expire.

- a** % arcdbutil sql
- b** Enter user-name: / as sysdba
- c** SQL> select PROFILE from dba_users where username =
'<arcsight_schema_owner>';
- d** SQL> alter PROFILE <profile result from step c> limit
PASSWORD_LIFE_TIME UNLIMITED;
- e** SQL> exit;

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

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

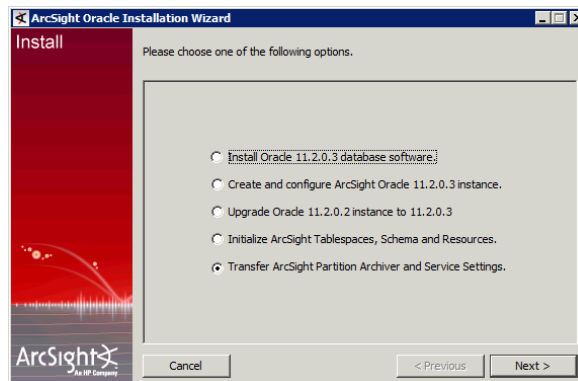
You have upgraded the ArcSight Database to 5.6. Go to the next section [Chapter 3, Upgrading Oracle Database, on page 17](#).

Transferring Partition Archiver Settings

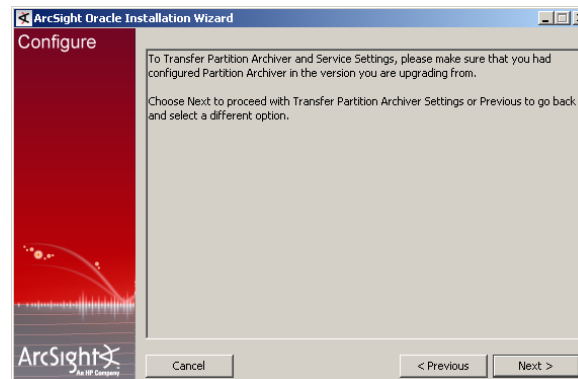


If you had partition archiving enabled and would like to disable the archiving now, check the Console for any partitions that have a reactivated status. If you see partitions with a reactivated status, deactivate them before disabling the Partition Archiver.

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



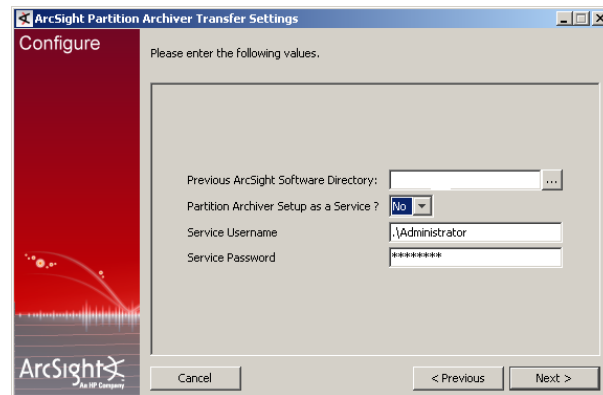
- 2 Click **Next** to confirm that you had configured the Partition Archiver in 5.5 (with the latest patch):



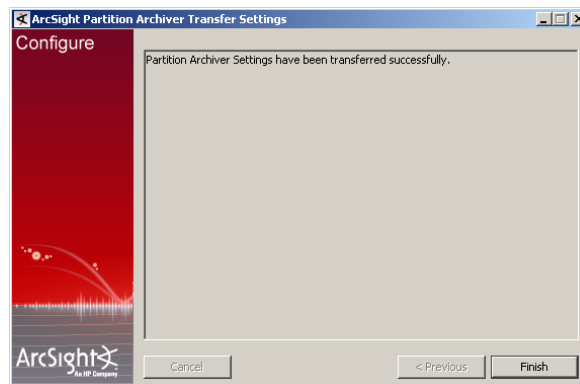
- 3 Enter the path name of the existing ArcSight Database's <ARCSIGHT_HOME> and **On Windows Only**, also enter your Windows Administrator's user name and password.

If you 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.
A message displays the successful transfer of Partition Archiver settings.
- 5 Click **Finish** in the screen shown below:



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

You have transferred Partition Archiver settings from your 5.5 (with the latest patch) database installation.



On Windows only: The Partition Archiver wizard prompts you in the last screen to install it as a service even though you might have chosen to not install it as a service. You may ignore this screen and exit.

Make sure to read the [“Notes about database upgrade and archives”](#) on page 12 and follow the instructions to enable dynamic sampling following it.

Chapter 3

Upgrading Oracle Database

You upgrade your Oracle database after you upgrade the ArcSight Database and before you upgrade the Manager. Before you begin, stop the Oracle database and take a cold backup of the entire database.



Making a cold backup of the database is an important precaution to ensure that you can go back to the previous version should something go wrong during the upgrade.

The following topics are covered:

[“Required Oracle Packages on x86 64-bit Linux” on page 17](#)

[“Before Upgrading to Oracle 11.2.0.4” on page 18](#)

[“Take a backup of all system resources and database definitions in your database. This backup is necessary in case the upgrade process fails. With it, you can restore your database to its original state and restart upgrade. Additionally, ArcSight-supplied resources are overwritten during the upgrade, so any changes you made are lost. To restore your changes after the upgrade, you can use the backup copy as a reference.” on page 19](#)

Required Oracle Packages on x86 64-bit Linux

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

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

On x86 64-bit Linux RHEL 5

```
binutils-2.17.50.0.6 (64-bit)
compat-libstdc++-33-3.2.3
gcc-4.1.2 (64-bit)
glibc-2.5-24 (both 32- and 64-bit)
glibc-common-2.5 (64-bit)
glibc-devel-2.5 (64-bit)
libaio-0.3.106 (both 32- and 64-bit)
libaio-devel-0.3.106 (both 32- and 64-bit)
```

```
libstdc++-4.1.2 (both 32- and 64-bit)
libstdc++-devel 4.1.2 (both 32- and 64-bit)
make-3.81 (64-bit)
sysstat-7.0.2 (64-bit)
unixODBC-2.2.11 or later (both 32- and 64-bit)
unixODBC-devel-2.2.11 or later (64-bit)
```

On x86 64-bit Linux RHEL 6.x

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

On SUSE Linux Enterprise Server 11

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

Before Upgrading to Oracle 11.2.0.4

Perform these preparatory steps to avoid upgrade failures:

- 1 Check if DST v17 is installed on your existing Oracle software. To do so, run the following command while logged in as the oracle user and check its output:

```
su - oracle
arcdbutil sql / as sysdba
select version from v$timezone_file;
exit;
```

If it returns 17, DST v17 has been installed; apply DST v17 for 11.2.0.4 after installing oracle 11.2.0.4 database software and before upgrading 11.2.0.3 oracle instance.

- 2 Take a backup of all system resources and database definitions in your database. This backup is necessary in case the upgrade process fails. With it, you can restore your database to its original state and restart upgrade. Additionally, ArcSight-supplied resources are overwritten during the upgrade, so any changes you made are lost. To restore your changes after the upgrade, you can use the backup copy as a reference.

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

- a Log in to the ArcSight Database system as the user who installed the ArcSight Database software (**oracle** on Linux 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 Linux and %<ORACLE_HOME>%\bin;%<PATH>% on Windows.
- c In <ARCSIGHT_HOME>/bin of your 5.5 (with the latest patch) 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.



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 a warning message in your command prompt or shell console window that says `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 5.5 (with the latest patch) database's <ARCSIGHT_HOME> directory.

- 3 Stop all the external Oracle sessions that are connected to the Oracle instance. This is required in order to upgrade the instance to Oracle 11.2.0.4.

- 4 Stop all Oracle services, for example, TNS Listener.
- 5 On Windows, stop the Distributed Transaction Coordinator service.
- 6 On Windows, verify that there are no processes holding up the <OrainstHome/BIN>/oci.dll file. If processes are calling the dll file, the upgrade program will be prevented from creating the installation directories.
- 7 If you had installed Oracle Enterprise Manager, stop it by running the following command from the ArcSight Database's bin directory:

```
emctl stop dbconsole
```

Upgrading Oracle



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

Upgrading the Oracle Software from 11.2.0.3 to 11.2.0.4

Upgrading Oracle from 11.2.0.3 to 11.2.0.4 has the following prerequisites:

- Stop all ESM component processes before you start this Oracle upgrade. That includes the Manager, Console, Partition Archiver, and ArcSight Web.
- If you configured your Oracle data storage within <ORACLE_HOME>, reconfigure the data storage to place these files elsewhere. If you do not reconfigure your data storage to place these files somewhere else, the upgrade might not be successful.

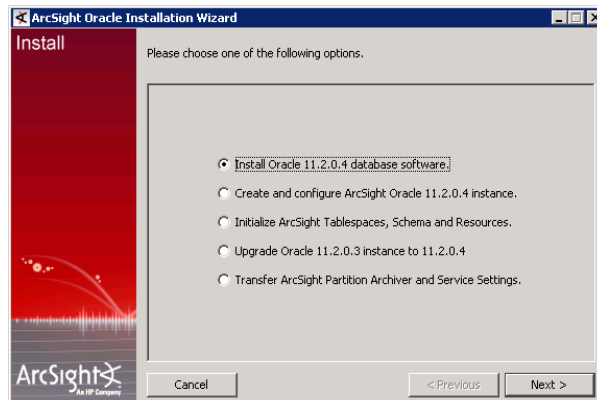
For information on finding and moving your database data files and Oracle Control files, look for the KCS articles "Moving Database Datafiles from One Disk to Another Local Disk or SAN Storage" and "How to relocate Oracle control files" on the HP SSO site at <http://support.openview.hp.com>. Search for KCS articles by name on the Self-Solve tab.

To upgrade your Oracle software from 11.2.0.3 to 11.2.0.4:

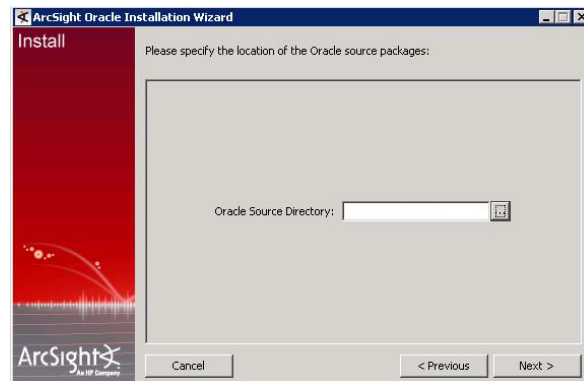
- 1 Run the following command from the bin directory of your ArcSight Database installation:

```
arcsight databasesetup
```

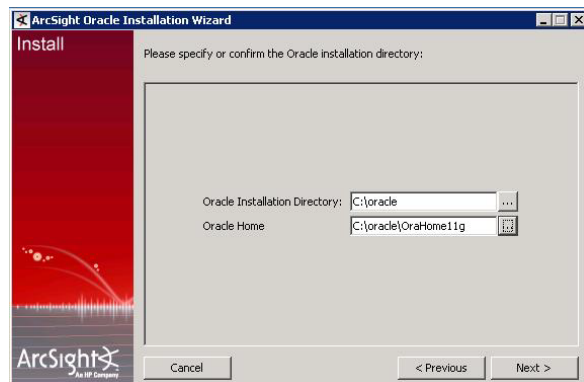
- 2 Select **Install Oracle 11.2.0.4 database software** and click **Next**.



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



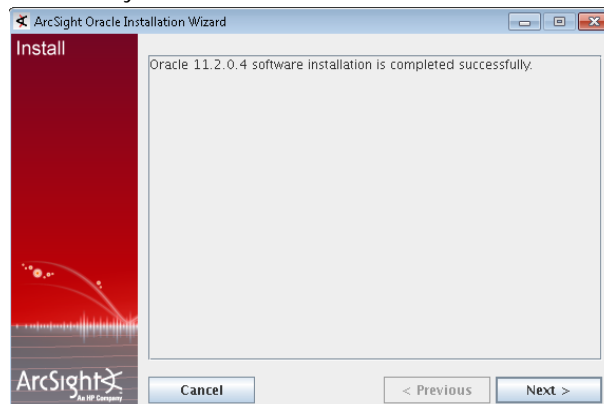
- 4 Enter the same file path for Oracle 11.2.0.4 as you used for 11.2.0.3, then click **Next**.



Caution

- Verify that the Oracle installation directory path and the <ORACLE_HOME> path do not contain any spaces.
- If you don't use the same file path as used in your 11.2.0.3 home, it might cause a failure in the upgrade that requires manual steps from HP Support to help you recover from the failure.

- 5 Review the pre-installation information and if satisfied, click **Next**.
- 6 The screen displays a message after the Oracle 11.2.0.4 software has been installed successfully. Click **Next**.



- 7 After you have completed Oracle 11.2.0.4 installation but before you start the upgrade, if you had installed Oracle Enterprise Manager (OEM) in Oracle 11.2.0.3 and want to upgrade the OEM, follow these steps:

On Linux:

While logged in as user "root", open another shell window and run the following two commands:



Note

If you don't know the hostname, go to \$ORACLE_HOME.backup/oc4j/j2ee and copy the entire folder name.

```
su - <OracleUserName> -c "cp -R
$ORACLE_HOME.backup/oc4j/j2ee/OC4J_DBConsole_
<hostname>_<sid>/ $ORACLE_HOME/oc4j/j2ee/"

su - <OracleUserName> -c "cp -R
$ORACLE_HOME.backup/<hostname>_<sid>/ $ORACLE_HOME"
```

On Windows:

- a You can use Windows Explorer to copy the following files:
- From <ORACLE_HOME>.backup\oc4j\j2ee\OC4J_DBConsole_<hostname>_<sid> and paste into <ORACLE_HOME>\oc4j\j2ee
 - From <ORACLE_HOME>.backup\<hostname>_<sid> and paste into <ORACLE_HOME>
- b Reboot your system, in order to allow access to the OEM URL.
- 8 **Only if you had the Daylight Savings Time patch (DST v17) installed on your Oracle software,**
- a Install DST v17 patch for 11.2.0.4 which you can obtain from the HP SSO website.
- b **On Windows only:** After applying the DST v17 patch, open <ORACLE_HOME>\oracore\zoneinfo\readme.txt and modify the "Current Content Version" to 17.

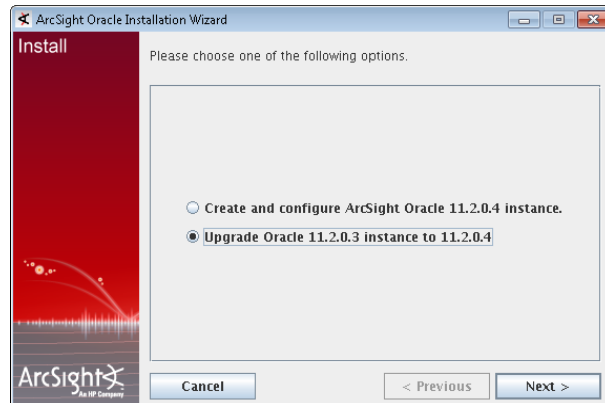
Upgrading the 11.2.0.3 Oracle Instance to 11.2.0.4



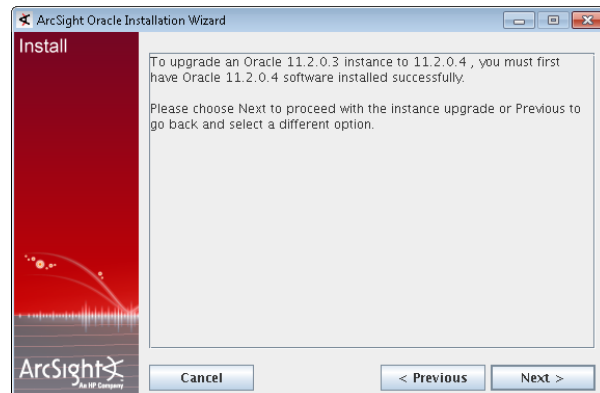
If you had installed the DST v17 Patch on 11.2.0.3, you must first install the DST v17 Patch by following [Step 8 on page 22](#) before proceeding with the Oracle upgrade, otherwise the upgrade will fail.

This topic continues from the previous steps.

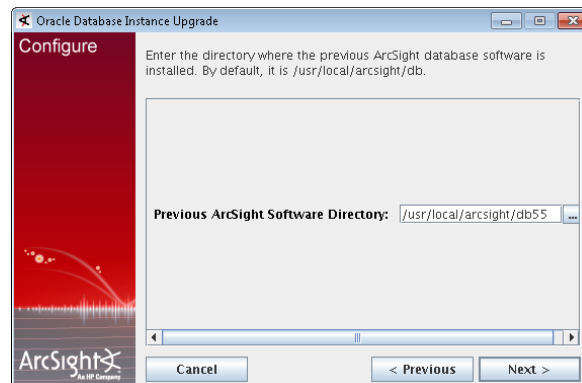
- 9 Select **Upgrade Oracle 11.2.0.3 instance to 11.2.0.4** and click **Next**.



- 10 Click **Next** if the Oracle 11.2.0.4 installation is successful.



- 11 Enter the location where your current ArcSight Database (5.5 with the latest patch) exists and click **Next**.



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

- 12 Enter the information about the previously-existing Oracle 11.2.0.3 software and click **Next**.

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

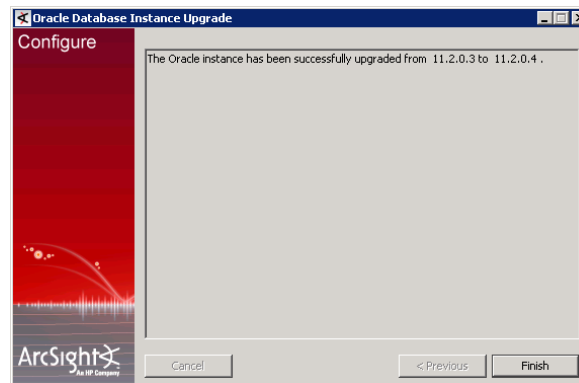


Note

Although you can install the Oracle Enterprise Manager client using HP's Oracle 11g Installer, you must acquire licensing and support from Oracle directly.

- 14 The next screen informs you that the instance upgrade is about to begin. Click **Next**.

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



You have upgraded your Oracle database and the instance to 11.2.0.4.

- 16 Verify that Oracle and the TNS Listener are now running.

Chapter 4

Upgrading ArcSight Manager

This chapter tells you how to upgrade your ArcSight Manager to 5.6. The following topics are covered here:

[“Upgrading the ArcSight Manager” on page 28](#)

[“Post-Upgrade Tasks” on page 37](#)

Preparing for the Manager Upgrade

These preparations should be performed before the Manager Upgrade, so do them now.

Prepare ArcSight Manager as follows:

- 1 Verify that your Manager machine is supported for 5.6. Refer to the Product Lifecycle document available on the HP ArcSight Customer Support website for the most current information on supported platforms.
- 2 If you downloaded the latest patch for your ArcSight Manager, install it.
- 3 Make a note of the details of your customized zones, such as the start and end addresses, their location in the directory hierarchy, and so on. It will come handy in case you need to restore the customization upon upgrade.
- 4 Make sure that you have run the `dbcheck` script on your database as described in [“Preparing the ArcSight Database Components” on page 9](#). After running `dbcheck`, make sure that all log files the script generates are error and warning free.
- 5 Archived partitions with archive type uncompressed should not be in reactivated state during Manager upgrade. Deactivate such partitions before you do the Manager upgrade.
- 6 Make sure that the Oracle service and TNS listener are running before upgrading the Manager.
- 7 If the Manager fails to start on RHEL, add the following line in your `/etc/profile` file:


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


and save the file. Then close all the sessions and logout and log back in.
- 8 By default, the heap size set for the upgrade process is 3 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 5.5 (with the latest patch) Manager. To do so,

- a Run the following command from your 5.5 (with the latest patch) 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 5.5 (with the latest patch) Manager.

On Windows:

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

This only affects the current command prompt window, so leave it open. Perform the Manager upgrade in this window when you get to it.

On Unix:

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

- e Make sure to run the upgrade from the same terminal session in which you set the ARCSIGHT_JVM_OPTIONS.

Upgrading the ArcSight Manager

**Note**

Do not upgrade ArcSight Manager until you have successfully upgraded ArcSight Database and successfully exported system tables as described in ["Preparing for the Manager Upgrade" on page 27](#).

**Note**

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 compressed 5.6 Manager installation file to a different machine, transfer it to your Manager system.
- 2 Extract the installation files from the compressed ArcSight-5.6.0.xxxx.0-Manager-<platform>.zip file.

**Note**

Upgrading ArcSight Web also requires you to extract its installation files from a compressed file. Installation files for ArcSight Web and ArcSight Manager should be **not** be present in the same folder. Make sure you do **not** extract the ArcSight Manager files into the folder where you plan to extract the ArcSight Web files.

- 3 Stop 5.5 (with the latest patch) Manager.

For instructions about stopping ArcSight Manager, see the ArcSight ESM Administrator's Guide.
- 4 Log in as user **arcsight** on Unix or the Administrator user on Windows on the Manager machine.

This step is required because for security reasons, the 5.6 Manager cannot be installed using the root user account.

5 Start the upgrade as appropriate for your platform:

◆ **On Windows:**

Double-click `ArcSight-5.6.0.xxxx.0-Manager-Win64.exe`

◆ **On Linux:**

Run the following command

```
./ArcSight-5.6.0.xxxx.0-Manager-Linux64.bin
```

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

```
./ArcSight-5.6.0.xxxx.0-Manager-Linux64.bin -i console
```

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

- ◆ **Introduction**—Read the introduction and click **Next**.
- ◆ **Installation Process Checklist**—Click **Next**.
- ◆ **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 then click **Next**.
- ◆ **Special Notice**—Read the notice and click **Next**.
- ◆ **Choose ArcSight Installation Directory**—Enter an `<ARCSIGHT_HOME>` path for 5.6 that is different from where the existing Manager is installed. Click **Next**.



Caution

Do not install ArcSight Manager 5.6 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.

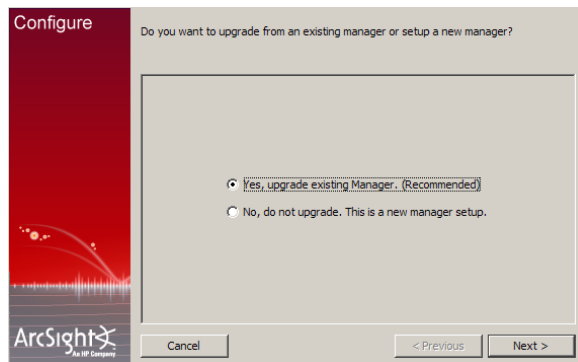
- ◆ **Choose Shortcut Folder** (on Windows) or **Choose Link Folder** (on UNIX). Specify or select where the ArcSight Manager icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows. Click **Next**.
- ◆ **Pre-Installation Summary**—Review the settings and click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



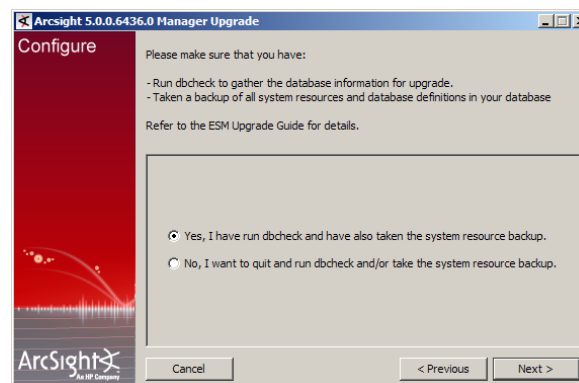
Caution

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 `arcsight upgrade manager` command from the ArcSight Manager 5.6's `\bin` directory in the same command window where you had set the manager's heap size in [Step d on page 28](#).

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



- 7 The next screen displays a message requesting you to make sure that you have a good understanding of all components before upgrading. Click **Next**.
- 8 If you did not run the `dbcheck` script on your database as described in [“Preparing the ArcSight Database Components” on page 9](#), run it and make sure that the log files that the script generates are error and warning free. Additionally, back up the system dump if you had not already done so.
- ◆ To stop the Manager upgrade, select **No, I want to quit and run dbcheck and/or take the system resource backup** and click **Cancel** in the following screen.



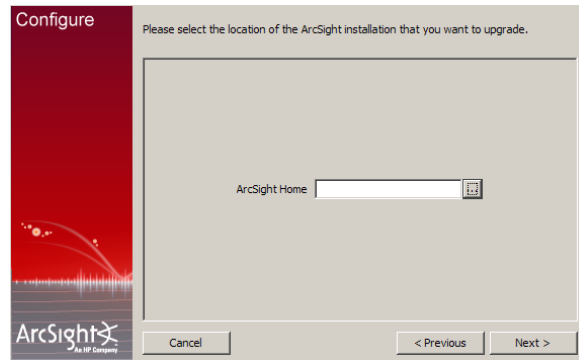
After you have run the `dbcheck` script, resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:

```
arcsight upgrade manager
```

The upgrade process resumes from this point.

- ◆ To continue with the Manager upgrade, select **Yes, I have run dbcheck and have also taken the system resource backup** and click **Next**.

- 9 Select the location of 5.5 (with the latest patch) 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 at [“To take a backup, export the system tables as follows:” on page 19](#). Then re-run the wizard through completion.

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



Resolve all duplicate names before proceeding further with the upgrade. Resolve duplicate names manually. Contact Customer Support using the HP SSO website if you need assistance.

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 ArcSight Database 5.6 installation's `<ARCSIGHT_HOME>/utilities/database/oracle/common/sql` directory to obtain a complete list of duplicate resource names:

```
cd ARCSIGHT_HOME/utilities/database/oracle/common/sql
<ARCSIGHT_HOME>/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 Customer Support using the HP SSO website.

- 11 The upgrade process also checks for archived partitions with archive type uncompressed that are in reactivated state. If you have such partitions, deactivate them before you proceeding with the Manager upgrade.

- 12 When you see the message that you have completed the first stage. Click **Next**.



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 5.5 (with the latest patch) system tables you exported in [“Preparing for the Manager Upgrade” on page 27](#) and then rerun:

```
arcsight upgrade manager
```

from the /bin directory of the location where you installed the 5.6 Manager.

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

```
arcsight import_system_tables <old_arcsight_user>  
<new_arcsight_user> <password> <db_instance>  
<dump_file_path> <dump_file_name>
```

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

At this point, the following changes have taken place:

- ◆ System tables are upgraded to 5.6.
- ◆ System indexes are upgraded to 5.6.
- ◆ Undelivered notifications are removed.
- ◆ User functions are upgraded.

ESM's content is installed as follows:



For an in-depth understanding of how resources installed with ArcSight ESM have been updated and rearranged, download the System Content Reference Guide from the Protect 724 download site.

- ◆ System Core content

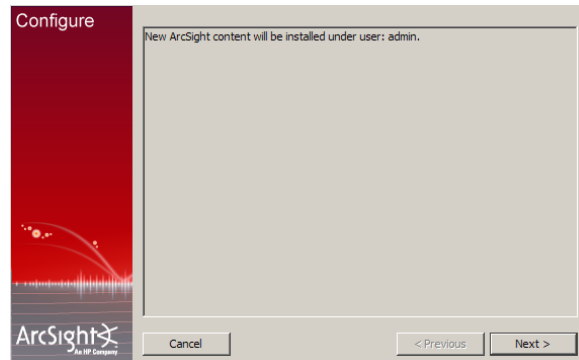
The System Core content provides the foundation building blocks for ArcSight ESM to work. This content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in /All Filters/ArcSight System/Core.

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

- ◆ Foundation content

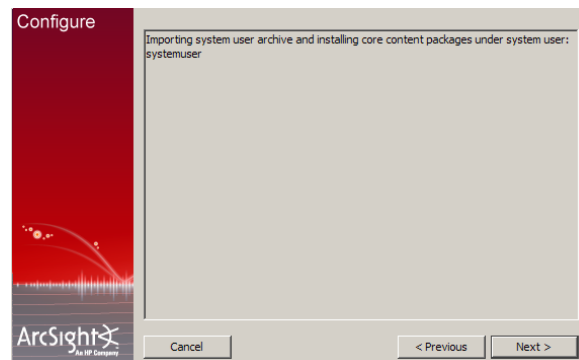
The Admin Foundation content is automatically installed as a part of ArcSight ESM to provide out-of-box resources that you can start using immediately to monitor and protect your network.

- 13 The screen states that the ArcSight Content packages will be installed under the user, admin. This is the user that owns the system content. Click **Next**:



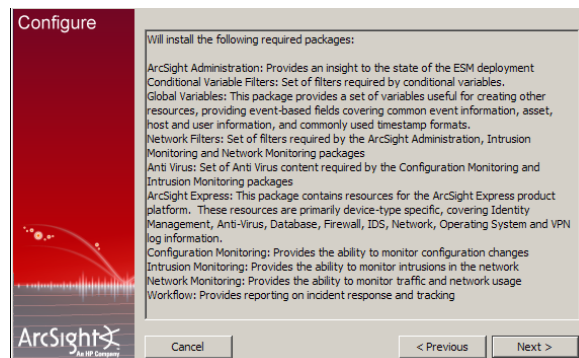
This step accomplishes the following:

- ◆ Enough cache size for resources is set.
 - ◆ ESM system content resources are upgraded.
- 14 The next dialog says that the core content packages are installing under systemuser. Click **Next**:

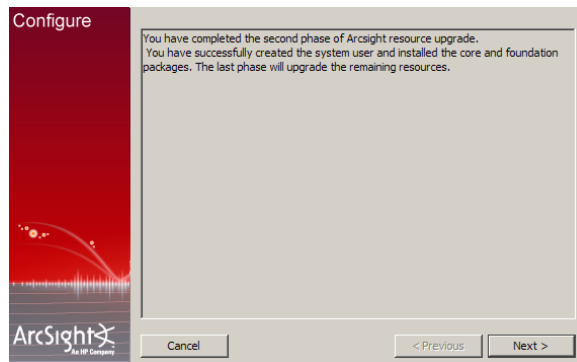


The system user is updated and the core content is installed.

- 15 The installer informs you that it will begin installing the required packages (Foundation content). Click **Next**.



- 16 You see the following screen when the content installation completes. Click **Next**.



The following happens:

- ◆ User's personal group is upgraded.
- ◆ Resource fix-up
- ◆ Viewer configuration is upgraded.
- ◆ The Database schema is updated to the latest version.

Resource validation

The next screen displays options for resource validation, a feature that allows you to validate a resource automatically. Some of the checks done are:

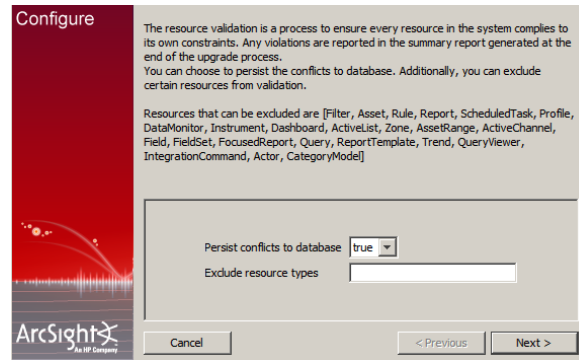
- ◆ Does a resource have valid values assigned to it?
For example, the validation process checks if an IP address assigned to an asset falls in the range of IP address assigned to the zone to which the asset belongs. If the IP address is outside the range, this discrepancy is listed in a report that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

You can choose to mark a resource as invalid (make it disabled) if the resource does not satisfy any checks. Or you may choose to get a report of all such resources and fix them manually later.

When a resource is marked invalid, 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 cannot participate in the event asset resolution. As a result, correlated events in which the source or target address points to the invalid asset are not generated. Similarly, if a rule is marked invalid, 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.



Validating resources

You can validate resources 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>
```

Use the same `ARCSIGHT_JVM_OPTIONS` as your 5.5 (with the latest patch) Manager when running this. See [Step d on page 28](#) for details on setting `ARCSIGHT_JVM_OPTIONS`.

If resource validation times out when running from the upgrade wizard, you can run it independently using the command mentioned in the tip above. Before doing so, update stats on the database by running the following command from the Database's `<ARCSIGHT_HOME>/bin`:

```
arcsight database ts -t nonpartitioned
```

Click **Next**.

- 17 If you had an ArcSight Web server set up for your 5.5 (with the latest patch) installation or you want to set up an ArcSight Web server for 5.6, 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 5.5 (with the latest patch) and do not want to set up one for 5.6, select **Do not enter URL for ArcSight Web** and click **Next**.

- 18 If you are setting up an ArcSight Web server for 5.6, 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, the port number is 9443.

- 19 Select whether you want to install the Manager as a service. The option you select from these Manager startup options takes effect when the Manager machine reboots.
- 20 On Unix platforms, if you get a message saying changes to the service configuration require root privileges, follow the steps listed on the message.
- 21 During the upgrade, the 5.5 (with the latest patch) `config/server/agentURLMapping.csv` file is saved with the file extension `.previous` in the `config/server` directory of 5.6 `<ARCSIGHT_HOME>`. If you customized this file in 5.5 (with the latest patch) and want to use it for 5.6, rename the saved file to remove the `.previous` extension. That is, rename `agentURLMapping.csv.previous` to `agentURLMapping.csv`.
- 22 On successful upgrade completion, you get a message to that effect. Click **Finish**.
- 23 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 5.5 (with the latest patch) to the 5.6 installation or fixing invalid resources.

HP 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. If it does not pop up, you can also access the report from `<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.

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

You have upgraded ArcSight Manager to 5.6.



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

- 25 Start the Manager.

Post-Upgrade Tasks

You are required to do the following after upgrading Manager to 5.6:

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

Use the same `ARCSIGHT_JVM_OPTIONS` as your 5.5 (with the latest patch) Manager when running this. See [Step d on page 28](#) for details on setting `ARCSIGHT_JVM_OPTIONS`.

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

```
arcsight refcheck -f true
```

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

- File resources are not handled properly during the ESM upgrade. This results in unassigned file resources after the upgrade. For example, the `.art` files are created as new file resources in ESM 5.5 (with the latest patch), and the resources 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 safely remove the unassigned `.art` files after an upgrade because they are duplicates.



The Manager updates the search index in the first few minutes after startup, so you may see a performance impact while the search index is being updated.

- After upgrading the Manager, you may see the following error in the `server.log` file after running the Manager for a few days:

```
Cannot allocate memory, not enough swap space.
```

This happens when externally-spawned processes have exceeded their allotted memory. If you see this error, search the logs for processes that are still running. Kill those processes manually.

For instructions about starting ArcSight Manager, see the 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 v5.6 Manager is complete, run the following command in `<ARCSIGHT_HOME>/bin` to start the Index Upgrade wizard. (Be sure to avoid running this from the Manager's `<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 set up Partition Archiver in your previous version, update Partition Archiver and start its service after upgrading ArcSight Manager. Completion of these steps upgrades the Partition Archiver version as viewed on the Console. With the Manager running:

- 1 Log in as the **oracle** user.
- 2 Run the following command from the Database `bin` directory to update the Partition Archiver:

```
arcsight agentsetup -w
```
- 3 Click **Next** on the few wizard screens until you get to the screen which asks you to either review or modify the parameters.
- 4 Select **I do not want to change any settings** and click **Next**.
- 5 Click **Finish** in the last screen.
- 6 **On Windows only:** You are prompted to enter the service information for the Partition Archiver. Click **Cancel**.
- 7 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 Linux:**

Run the following command:

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



`arc_oraclepartitionarchiver_db` is the default service name.

- 8 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 archiving is archived as expected.



If you start Partition Archiver after an Oracle upgrade, you may run into Partition Archiver-related issues. If you do, run the `arcsight database pc` command. See the ESM Administrator's Guide for details about this command, and the ESM Installation and Configuration Guide for details about Partition Archiver.

Chapter 5

Upgrading ArcSight Console

This chapter describes how to upgrade your ArcSight Consoles.

This upgrade process should be performed on all ArcSight Console instances that are to connect to the upgraded ArcSight Manager 5.6.

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



On Macintosh platforms only: If your Macintosh automatically updates the JVM to version 1.6.0_26, copy the old cacerts file from the previous JVM installation to the most recent JVM location. The cacerts file is located at: `/System/Library/Java/JavaVirtualMachines/1.6.0_jdk/Contents/Home/lib/security`, which points to `/System/Library/Java/Support/CoreDeploy.bundle/Contents/Home/lib/security`. If you don't have a backup of the cacert file, please contact the Customer Support using the HP SSO website.

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 5.6 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-5.6.0.xxxx.0-Console-Win.exe`

◆ **On Macintosh:**

Run the following command.

```
./ArcSight-5.6.0.xxxx.0-Console-MacOSX.zip
```

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

```
./ArcSight-5.6.0.xxxx.0-Console-MacOSX.zip -i console
```

◆ **On Linux:**

Run the following command.

```
./ArcSight-5.6.0.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-5.6.0.xxxx.0-Console-Linux.bin -i console
```

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

- ◆ **Installation Process Check**—Click **Next**.
- ◆ **Introduction**—Read the Introduction and click **Next**.
- ◆ **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 then click **Next**.
- ◆ **Special Notice**—Read the notice and click **Next**.
- ◆ **Choose Installation Folder**—Enter an <ARCSIGHT_HOME> path for 5.6 that is different from where the existing Console is installed.



Do NOT install 5.6 Console in the same location as the existing Console.

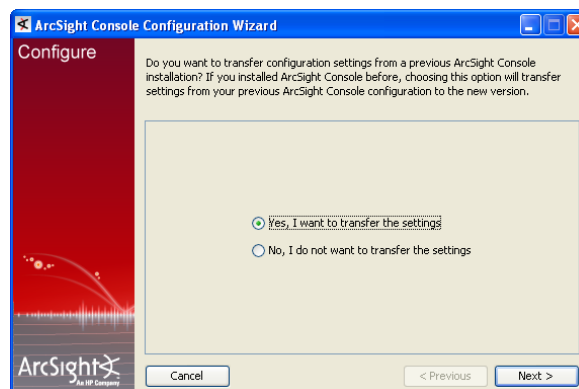
Caution

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

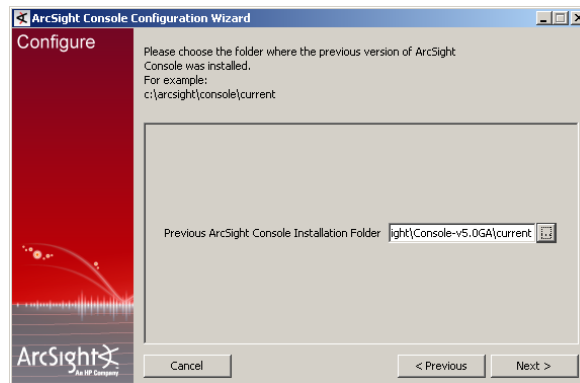
- ◆ **Choose Shortcut Folder** (on Windows) or **Choose Link Folder** (on Linux)—Specify or select where the ArcSight Console icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows. Click **Next**.
- ◆ **Pre-Installation Summary**—Review the settings and click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

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

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



- 5 You are 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 above.

Click **Next**.

- 6 See the ESM Installation and Configuration Guide for details on the remaining screens for installing a Console using the installation wizard.
- 7 Start the ArcSight Console.
- 8 After you have upgraded a Console to 5.6:
 - 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.
- 9 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 Customer Support through the HP SSO website.

Chapter 6

Upgrading ArcSight Web

This chapter describes how to upgrade your ArcSight Web to 5.6.



The list of supported platforms for ArcSight Web 5.6 is same as the one for ArcSight Manager 5.6.

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

Perform the following steps to upgrade your ArcSight Web.

- 1 Make sure that your Manager is up and running.
- 2 Stop the current ArcSight Web if it is running.
- 3 If you downloaded the compressed ArcSight Web 5.6 installation file to a different machine, transfer it to your ArcSight Web machine.
- 4 Extract the installation files from the compressed ArcSight-5.6.0.xxxx.0-Web-<platform>.zip file.



Upgrading ArcSight Web also requires you to extract its installation files from a compressed file. Installation files for ArcSight Web and ArcSight Manager should be **not** be present in the same folder. Do **not** extract the ArcSight Web files into the folder where you have extracted the ArcSight Manager files.

- 5 Start the installation as appropriate for your platform:

- ◆ **On Windows:**

Double-click ArcSight-5.6.0.xxxx.0-Web-Win.exe

- ◆ **On Linux:**

Run the following command.

```
./ArcSight-5.6.0.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-5.6.0.xxxx.0-Web-Linux.bin -i console
```

- 6 Step through the Installation Wizard screens. Specifically, enter values as described below for the following Wizard screens:
 - ◆ **Introduction**—Read the introduction and click **Next**.
 - ◆ **Installation Process Checklist**—Click **Next**.
 - ◆ **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 then click **Next**.
 - ◆ **Special Notice**—Read the notice and click **Next**.
 - ◆ **Choose Installation Folder**—Enter an <ARCSIGHT_HOME> path for 5.6 that is different from where the existing Web is installed.



Do NOT install ArcSight Web 5.6 in the same location as the existing ArcSight Web.

Caution

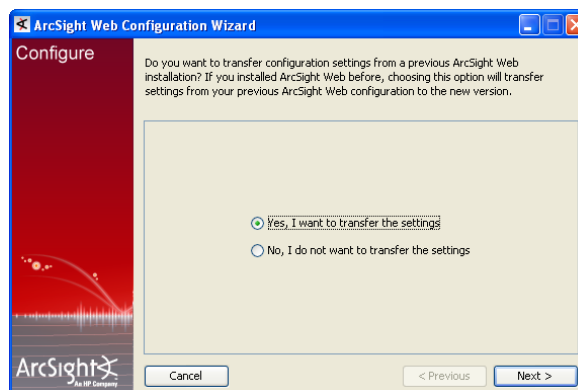
Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder** (on Windows)/**Choose Link Folder** (on Linux)—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**.

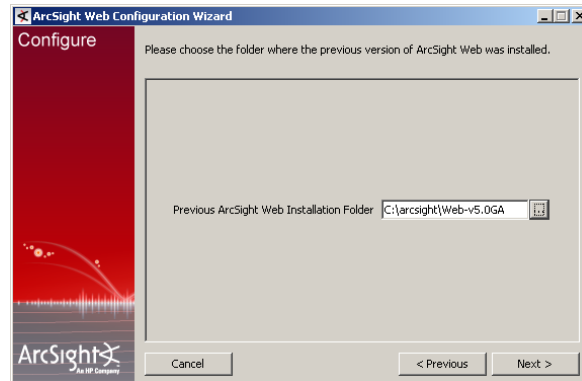
After you have stepped through the Installation wizard, it automatically starts the Configuration wizard.

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

Select your preferred option, then click **Next**.



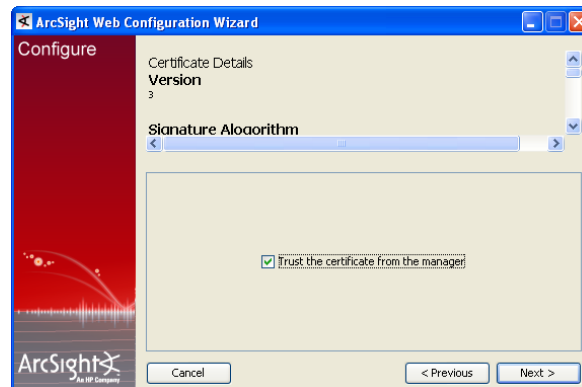
- 8 If you selected **Yes, I want to transfer the settings**, the ArcSight Web installation program prompts you to enter the location for your previous installation.



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 are prompted to select the mode in which you are upgrading after you click **Next**.

- 9 Follow the prompts in the few subsequent screens.
- 10 When prompted to trust the Manager's certificate, check the box as shown in the following screen.



- 11 Continue with the upgrade by following in 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.

- 12 Start ArcSight Web.

Checking the State of Existing Content after the Upgrade

After the upgrade is completed, verify that all your content has been successfully transferred to the 5.6 structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

- **Check for resources under Unassigned.** 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 5.5 (with the latest patch) *System* group.

If you find resources in them, move them to other custom groups, as appropriate. HP recommends against moving these resources into any ArcSight standard content groups, because they will be moved again to the Unassigned group during future upgrades.
- **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 from the backed up version you had saved before upgrade.
- **Check for assets under Disabled.** 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 the upgrade, check 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 5.6. This may happen for assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In 5.6, 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 the upgrade, verify that your user ACLs are correct and still valid based on how ArcSight standard content is organized for 5.6. For example, Administrator access should only be granted to those with authority to work with system-level content, such as for ArcSight System and ArcSight Administration. Update user ACLs manually as appropriate.

- **Zones resource.** Check if any zones were invalidated during the upgrade process.
 - ◆ Fix zones that you want to keep but may have been rendered invalid during the upgrade.
 - ◆ Verify that the assets assigned to zones that have been moved or invalidated during the upgrade retain their connections to the appropriate 5.5 (with the latest patch) zones.
 - ◆ Delete any invalid zones that you no longer want to keep.
 - ◆ If you had made customizations to the existing standard zones, manually edit the new resource to restore the customizations you had made to the corresponding 5.6 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, to 5.5 (with the latest patch) and are now upgrading to 5.6), 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, 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 and may not work as expected.

As an example, 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 on work as expected, run 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 5.6, 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.

■ Deprecated Resources and Resource Groups

Some of the ESM 3.x resources and resource groups have been deprecated, meaning they are no longer needed. Resources are deprecated for several reasons:

- ◆ The resource was too product- or vendor- specific.
- ◆ The resource was inefficient, or presented marginal value (for example, a collection of 10 reports was really one report with nine small variations).
- ◆ New 5.6 features accomplish the same goal more efficiently.

During the upgrade, resources that have been deprecated are moved to a separate `Deprecated` group for that resource type. The resources that are moved into it retain the hierarchy they had in their original ESM 3.x form. Resources moved to this folder are still active, so if you rely on any of these resources, they will still be present and operational.



Note

If you have built resources that refer to a deprecated resource, or if you have modified a deprecated resource to refer to a resource that has not been deprecated, some connections could be broken during upgrade.

If you still need to use the deprecated resource, resolve the broken reference by moving the deprecated resource back into the active resource tree and changing the conditions as needed.

If you no longer need the deprecated resources, you can safely delete them after the upgrade.

If you still rely on a deprecated resource, you can move it back into an active resource tree and modify its conditions, as necessary, to repair any broken references.



Note

HP no longer supports deprecated resources, so if you choose to restore a deprecated resource, you are responsible for its maintenance.

HP also recommends that you verify whether the new 5.6 resources address the same goal more efficiently.

After ESM 5.6 is installed, you can generate a list of deprecated resources using the Find Resource function:

- 1 In the ArcSight Console, go to **Edit > Find Resource**.
- 2 In the Search Query field, enter the keyword **deprecated** and click **Find**.

Upgrading ArcSight SmartConnectors

At a minimum, the SmartConnectors must be running version 3.1.0.4021.0. However, HP 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 HP SSO download site for details.

Download installation files as appropriate for your SmartConnector platforms. To leverage the ESM 5.6 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](#).

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 ESM fields.

Upgrading the Forwarding Connector

Refer to the ArcSight Forwarding Connector Configuration Guide for instructions on how to upgrade your Forwarding Connector.



When upgrading the Forwarding Connector, if FIPS mode is enabled for the Forwarding Connector, you do not need to re-import the Manager certificate upon Forwarding Connector upgrade.

Upgrading Hierarchical or Other Multi-Manager ESM Installations to 5.6

This chapter describes the method for upgrading a multi-ArcSight Manager deployment from 5.5 (with the latest patch) to 5.6.

Summary

In a multi-ArcSight Manager deployment, two or more ArcSight Managers are deployed in one of the following configurations:

- In a hierarchy—Data from one or more source Managers is forwarded to a central, destination Manager.
- In a High Availability (failover) configuration—An alternate instance of a Manager is on standby, ready to take over if the active Manager is unavailable.
- In a peer-to-peer configuration—Data from a SmartConnector is sent to more than one independent Managers for redundancy.

The process of upgrading ESM components—Database, Manager, Consoles, ArcSight Web, and SmartConnectors—in a multi-Manager deployment is similar to upgrading components in a single-Manager deployment. However, you upgrade the destination Managers and databases first, then the components connected to them, followed by the standby or source Managers and databases. ArcSight Forwarding Connectors must be upgraded only after their Managers have been upgraded. The Forwarding Connectors must be the version that shipped with ESM, or the latest version.

Upgrading a Hierarchical Deployment

To upgrade a hierarchical deployment, follow these steps starting at the destination Manager.

- 1 Upgrade any SmartConnectors that are not running a recent version. For best results, use version 4.8.1 or later.
- 2 Stop your current Manager.
- 3 Follow instructions in the [“Upgrading ArcSight Database Components” on page 9](#) to upgrade your ArcSight Database to 5.6.
- 4 Follow instructions in the [“Upgrading ArcSight Manager” on page 27](#) to upgrade your Manager to 5.6.
- 5 Start the ArcSight Manager 5.6.

- 6 Once the Manager 5.6 is running, follow instructions in the [“Upgrading ArcSight Console” on page 41](#) to upgrade any Consoles connected to it.
- 7 Upgrade the Forwarding Connector connected to this manager to build
`ArcSight-5.1.5.6973.0-SuperConnector-<platform>.<extension>`.

If the Forwarding connector is connected to more than one destination Manager, upgrade all such Managers before upgrading the Forwarding Connector.

Repeat this procedure until all Managers and Forwarding Connectors at each level of the hierarchy are upgraded.

Upgrading a High Availability (Failover) Configuration

In a High Availability (HA) configuration, the active and the standby Managers can share the database and the installation directory. See the technical note, “Deploying ArcSight ESM for High Availability,” available on the HP SSO website for more information on deploying ESM for high availability.

In preparation for upgrading your ESM components, follow the procedure recommended by your third-party failover management software vendor to allow for software updates. Refer to their documentation for steps on how to upgrade your HA configuration.

For instructions on how to upgrade the ESM components, refer to the technical note that applies to your upgrade path.

Upgrading a Peer-to-Peer Configuration

To upgrade a setup in which SmartConnectors send data to more than one Manager directly—that is, two or more Managers are peers—follow the upgrade process described in the upgrade technical note that applies to your upgrade path, for one of the Managers followed by the other Managers.

Index

A

- ArcSight Database
 - preparing to install 9
 - supported platforms 9

- upgrading

- ArcSight Console 41

C

- cold backup 17

D

- database check 10
- database components 9

E

- excluding
 - resources to validate 35

H

- heap size 27

I

- Index, upgrading 37
- invalid resources 50
- IO transfer speed 13

O

- Oracle packages 17

P

- Partition Archiver service 11
- platforms, supported for Manager 27

R

- redundant name check 31
- resource validation 34

S

- SmartConnectors 53
- system resources, backup 19
- system tables 19

U

- updating
 - Partition Archiver service 38

