# Upgrading ArcSight™ ESM

## v5.0 SP1 or v5.0 SP2 to v5.2

March 2012

ArcSight™
An HP Company

**Upgrading**
**ArcSight™ ESM v5.0 SP1 or v5.0 SP2 to v5.2**

Copyright © 2012 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.arcsight.com/copyrightnotice

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

This document is confidential.

## Revision History

| Date | Product Version | Description |
|---|---|---|
| 03/01/2012 | Upgrading ArcSight ESM | v5.0 SP1 and v5.0 SP2 to v5.2 |

## Contact Information

| | |
|---|---|
| **Phone** | 1-866-535-3285 (North America)<br>+44 (0)870 141 7487 (EMEA) |
| **Support Web Site** | http://support.openview.hp.com |
| **Protect 724 Community** | https://protect724.arcsight.com |

# Contents

Chapter 1

# Preparing for Upgrade

This technical note describes the steps required to upgrade the ArcSight ESM components from v5.0 SP1 or v5.0 SP2 to v5.2.

If you are upgrading from ESM 5.0 SP2 Patch 2 to ESM 5.2, you will not be able to benefit from some of the fixes available in ESM 5.0 SP2 Patch 2 after you upgrade to v5.2. ESM v5.2 does not include the fixes made in v5.0 SP2 Patch 2. However, you can get these fixes when ESM 5.2 Patch 1 becomes available. Please refer to the ESM 5.0 SP2 Patch 2 release notes to see the list of these fixes.

When upgrading, you must upgrade in the same mode (FIPS or default) as the mode of your current ESM installation. For example, if you are upgrading an ESM installation that is currently running in FIPS mode, you must upgrade that ESM installation in FIPS 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:

Downloading Installation Files, Scripts, and Other Documents

Downloading Installation Files, Scripts, and Other Documents

Upgrading ArcSight Database Components

Upgrading ArcSight Manager

Upgrading ArcSight Console

Upgrading ArcSight Web

Checking the State of Existing Content After Upgrade

Upgrading ArcSight SmartConnectors


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.

If you have a hierarchical or a multi-Manager ESM setup, also see "Upgrading Hierarchical or Other Multi-Manager ArcSight™ ESM Installations to v5.2" on page 47.

# 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 HP support website.

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 v5.2 files for all components as listed below 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 v5.2 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 5.0.1.xxxx.n format for v5.0 SP1 and 5.0.2.xxxx.n format for v5.0 SP2, 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-5.2.0.xxxx.0-DB-Win.exe`
   - `ArcSight-5.2.0.xxxx.0-DB-AIX.bin`
   - `ArcSight-5.2.0.xxxx.0-DB-Linux.bin`
   - `ArcSight-5.2.0.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 Console that connects to the Manager, click **Help** | **About**. The current version is displayed in 5.0.1.xxxx.n format for v5.0 SP1 and 5.0.2.xxxx.n format for v5.0 SP2, 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-5.2.0.xxxx.0-Manager-Win.zip`
   - `ArcSight-5.2.0.xxxx.0-Manager-Win64.zip`

- ArcSight-5.2.0.xxxx.0-Manager-AIX.zip
- ArcSight-5.2.0.xxxx.0-Manager-Linux.zip
- ArcSight-5.2.0.xxxx.0-Manager-Linux64.zip
- ArcSight-5.2.0.xxxx.0-Manager-Solaris.zip

**For the Consoles:**

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

- ArcSight-5.2.0.xxxx.0-Console-Win.exe
- ArcSight-5.2.0.xxxx.0-Console-Linux.bin
- ArcSight-5.2.0.xxxx.0-Console-MacOSX.zip

**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-5.2.0.xxxx.0-Web-Win.zip
- ArcSight-5.2.0.xxxx.0-Web-AIX.zip
- ArcSight-5.2.0.xxxx.0-Web-Linux.zip
- ArcSight-5.2.0.xxxx.0-Web-Solaris.zip

**Other Documentation:**

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

- ArcSight ESM v5.2 Release Notes
- ArcSight ESM Installation and Configuration Guide
- ArcSight ESM Administrator's Guide
- ArcSight ESM System Content Reference Guide

These documents are available on the HP SSO download site.


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 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.

# 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 ESM Console User's Guide topic "Managing Resources > Managing Packages". In some cases, modifications you have made to existing ArcSight resources may need to be

reconfigured manually after the upgrade, and 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 upgrade, existing assets upgrade seamlessly.

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

- **Zones Resource**. Zones are used by ArcSight to identify the network devices that contribute to the event stream by their IP addresses.
  - If you made customizations directly to the standard ESM zones (with the original resource ID), the customizations you made will be overwritten during the upgrade. Be sure to back up these customizations so you can restore them manually after the upgrade.
  - If you created your own zones, any that overlap standard ArcSight zones are disabled and placed in the Disabled Zones group.
  - Before 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 5.2.

## Upgrading the Oracle Software

ESM v5.2 does not support Oracle 10.2.0.4. If you are using Oracle 10.2.0.4, you must upgrade your Oracle instance to 11.2.0.2. You can do so using the ESM v5.0 SP2 ArcSight Database installer. Refer to the ESM v5.0 SP2 Upgrade Guide for detailed instructions on upgrading the Oracle software.

If you are currently using Oracle 11.2.0.1, you must first upgrade your Oracle software to 11.2.0.2 by upgrading to ESM v5.0 SP2 patch2 before upgrading to v5.2. Refer to the ESM v5.0 SP2 Patch2 release notes for detailed instructions to do so.

## 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 v5.2.

| Operating System | Database | Typical System Configuration |
|---|---|---|
| Microsoft Windows Server 2003 R2 (SP2) 32-bit<br>Microsoft Windows Server 2003 R2 (SP2) 64-bit<br>Microsoft Windows Server 2008 R2 SP2 64-bit | Oracle 11.2.0.2 | x86-compatible multi-CPU system with 2-16 GB RAM |

| Operating System | Database | Typical System Configuration |
|---|---|---|
| Red Hat Enterprise Linux 5 (RHEL 5.7) 32-bit<br>Red Hat Enterprise Linux 5 (RHEL 5.7) 64-bit<br>Red Hat Enterprise Linux 6.1 64-bit<br>SUSE Linux 11 Enterprise Server 64-bit | Oracle 11.2.0.2 | x86-compatible multi-CPU system with 2-16 GB RAM |
| Sun Solaris 10, 64-bit<br>Sun Solaris 11, 64-bit | Oracle 11.2.0.2 | Sparc-compatible multi-CPU system with 2-16 GB RAM |
| IBM AIX 5L, Version 5.3 (5.3.0.70) 64-bit<br>IBM AIX 6L, 6.1 64- bit | Oracle 11.2.0.2 | pSeries system with 2-16 GB RAM |


Refer to the ArcSight ESM Product Lifecycle document available on the Protect 724 website 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 Perform these steps to identify if your v5.0 SP1 or v5.0 SP2 database is ready for upgrade:

a Shut down your currently installed v5.0 SP1 or v5.0 SP2 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 SP1 or v5.0 SP2 database installation, run the following command:

On Windows:

```
arcsight dbcheck
```

On Unix:

```
./arcsight dbcheck
```

You will see the following files 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.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, contact Customer Support via the HP SSO website and be prepared to send the dbchecklogs.tar.gz or dbchecklogs.zip file (as appropriate for your platform) to them if requested.

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


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

# Upgrading the ArcSight Database Software, and Partition Archiver

1 Make sure to close any open connections to Oracle database before proceeding further.

2 If you downloaded the v5.2 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-5.2.0.xxxx.0-DB-Win.exe

- **On Solaris**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-DB-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-DB-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-DB-Linux.bin -i console
  ```

The installer launches the Introduction window.

6 Click **Next** in the Introduction screen.

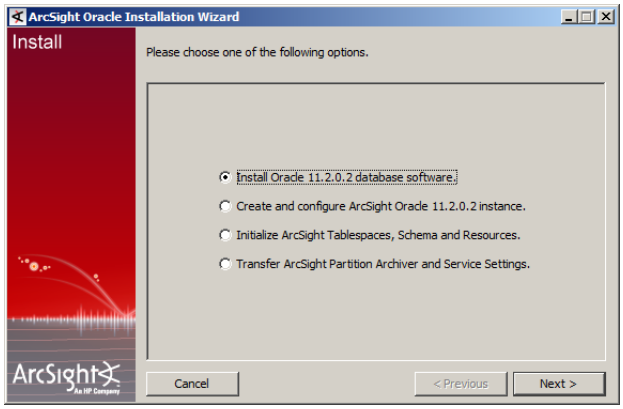
7 In the License Agreement screen, read the agreement text and click **I accept the terms of the License Agreement** radio button and click **Next**. This radio button will be disabled until you scroll to the bottom of the agreement to help ensure that you have read the agreement.

8 Read the Special Notice and click **Next**.

9 Enter the location where you want to install the v5.2 database software. This location should be different from the location where you have the v5.0 SP1 or v5.0 SP2 database software installed. Click **Next**.

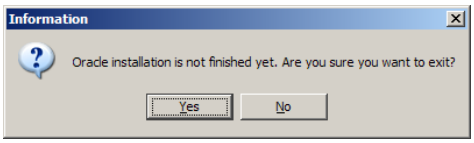
10 Review the pre-installation summary and click **Install**.

11 Select an option in the following screen to suit your needs based on the description below and click **Next**.




- Click **Cancel** if:
  - you do not want to upgrade your Oracle installation and/or
  - you did not have Partition Archiver configured in v5.0 SP1 or v5.0 SP2

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




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

Note

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 SP1 or v5.0 SP2, you will need to transfer the Partition Archiver settings to your v5.2 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 15 for details on the wizard screens that follow.

Note

**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 v5.2. See the section, "Updating and Starting the Partition Archiver Service" on page 32 in the Upgrading ArcSight Manager chapter.
- If you have archived partitions and you had set up your Partition Archiver to archive with type uncompressed, backup 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
```


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

You have upgraded the ArcSight Database v5.2 software. Go to the next section Upgrading ArcSight Manager.

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

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

a `% arcdbutil sql`

b Enter user-name: `/ as sysdba`

c SQL> `select PROFILE from dba_users where username = '<arcsight_schema_owner>';`

d SQL> `alter PROFILE <profile result from step 3>  limit PASSWORD_LIFE_TIME UNLIMITED;`

e SQL> `exit;`

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

a % `arcdbutil sql`

b Enter user-name: `/ as sysdba`

c SQL> `alter user <arcsight_schema_owner> account unlock;`

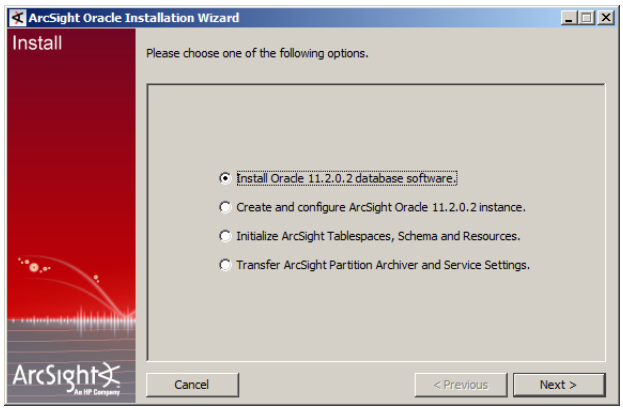
d SQL> `exit;`

For more information on changing this behavior, refer to the knowledge base article KB 5205, which is available from the ArcSight support portal at https://support.arcsight.com.

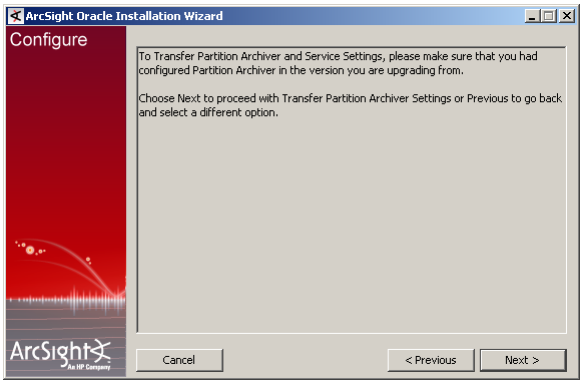
# Transferring Partition Archiver Settings


If you had partition archiving enabled and would like to disable the archiving now, you must check the Console for any partitions that have a reactivated status.If you see partitions with a reactivated status, you need to deactivate those partitions 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 v5.0 SP1 or v5.0 SP2:

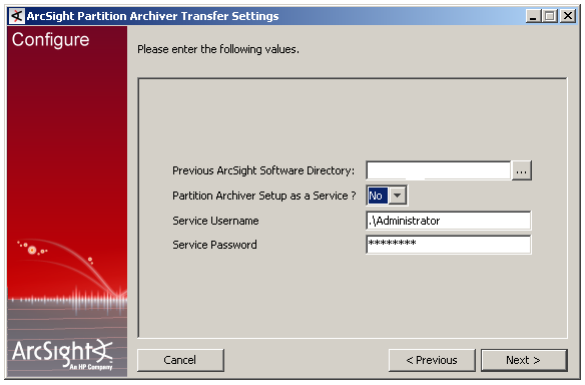



3 Enter the path name of the existing ArcSight Database's `<ARCSIGHT_HOME>` and

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

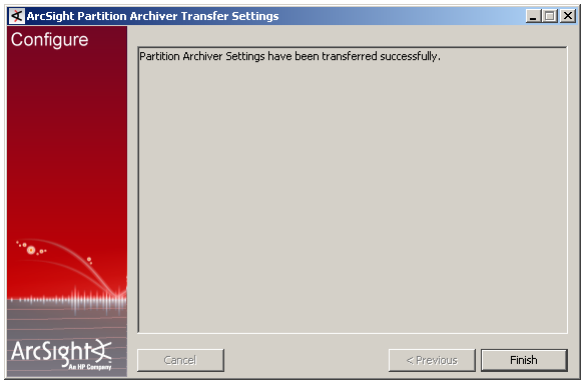
If you had set up the Partition Archiver as a service in your previous installation, select **Yes** from the **Partition Archiver as a service?** drop-down list, otherwise select **No**.

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 SP1 or v5.0 SP2 Database installation.

**Note**

**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. Please ignore this screen and exit out of it.

Make sure to read the "Notes about database upgrade" on page 13 and follow the instructions to enable dynamic sampling following it.

# Post-Upgrade Steps on AIX Platform Only

Run the following commands that are required in order for the Partition Archiver to function as expected:

```
./arcdbutil sql

SQL>conn / as sysdba

SQL>ALTER SYSTEM set filesystemio_options=ASYNCH scope=spfile;

SQL>shutdown immediate;

SQL>startup
```

```
SQL> show parameter filesystemio_options

//output should print ASYNCH as the value

SQL>exit
```

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 v5.2 from the list of supported platforms and database versions in "Preparing the ArcSight Database Components" on page 9.
2. Verify that your Manager machine is supported for v5.2 from the list of supported platforms in the following table.


Make sure that you use the 64-bit installer when upgrading the Manager on a 64-bit platform. On a 32-bit platform, use the 32-bit installer.

| Platform | Supported Operating System | Typical System Requirements |
|---|---|---|
| Linux | Red Hat Enterprise Linux (RHEL) 5.7 32-bit<br>Red Hat Enterprise Linux (RHEL) 5.7 64-bit<br>Red Hat Enterprise Linux (RHEL) 6.1 64-bit<br>SUSE Linux 11 Enterprise Server 64-bit | x86-compatible multi-CPU system with 4 GB RAM |

| 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<br>Microsoft Windows Server 2008 R2 64-bit | x86-compatible multi-CPU system with 4 GB RAM |
| Solaris | Sun Solaris 10 (10/09) 64-bit<br>Sun Solaris 11 64-bit | Sparc-compatible multi-CPU system with 4 GB RAM |
| IBM AIX | IBM AIX 5L, Version 5.3 (5.3.0.70) 64-bit<br>IBM AIX, Version 6.1 64-bit | pSeries system with 4-16 GB RAM |


Refer to the ArcSight ESM Product Lifecycle document available on the HP SSO website 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 9. After running `dbcheck`, make sure that all log files the script generates are error and warning free.

6 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 ('oracle' 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 SP1 or v5.0 SP2 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.


- 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 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 SP1 or v5.0 SP2 Database's `<ARCSIGHT_HOME>` directory.

**8** Make sure that the TNS listener is running before upgrading the Manager. To check the TNS listener,

On Windows machines, check the status of the TNSListener service in the Services window of Administrative Tools.

On Unix machines run this command on the database machine:

```
% arcdbutil lsnrctl status
```

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

```
% arcdbutil lsnrctl start
```

**9** On RHEL 5.7, 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.

**10** By default, the heap size set for the upgrade process is 1.5 GB on 32 bit machines and 3 GB on 64-bit machines. 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 SP1 or v5.0 SP2 Manager. To do so,

**a** Run the following command from your v5.0 SP1 or v5.0 SP2 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 SP1 or v5.0 SP2 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 22.

**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 19.


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 v5.2 Manager installation file to a different machine, transfer it to your Manager system.

2 Extract the installation files from the compressed `ArcSight-5.2.x.nnnn.y-Manager-<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. So, make sure that you do **not** extract the ArcSight Manager files into the folder where you plan to extract the ArcSight Web files.

3 Make sure that the v5.0 SP1 or v5.0 SP2 Manager is stopped.

For instructions about shutting down your ArcSight Manager, see 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 the v5.2 Manager cannot be installed using the "root" user account for security reasons.

5 Start the upgrade as appropriate for your platform:

- **On Windows**:

  For 32-bit host:

  Double-click `ArcSight-5.2.0.xxxx.0-Manager-Win.exe`

  For 64-bit host:

  Double-click `ArcSight-5.2.0.xxxx.0-Manager-Win64.exe`

- **On Solaris**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Manager-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Manager-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command for 32-bit host:

  ```
  ./ArcSight-5.2.0.xxxx.0-Manager-Linux.bin
  ```

  Run the following command for 64-bit host:

  ```
  ./ArcSight-5.2.0.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.

  On 32-bit machines, run:

  ```
  ./ArcSight-5.2.0.xxxx.0-Manager-Linux.bin -i console
  ```

  on 64-bit machines, run:

  ```
  ./ArcSight-5.2.0.xxxx.0-Manager-Linux64.bin -i console
  ```

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

- **Installation Process Checklist**—Click **Next**.
- **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 then click **Next**.
- **Special Notice**—Read the notice and click **Next**.

- **Choose ArcSight Installation Directory**—Enter an `<ARCSIGHT_HOME>` path for v5.2 that is different from where the existing Manager is installed. Click **Next**.

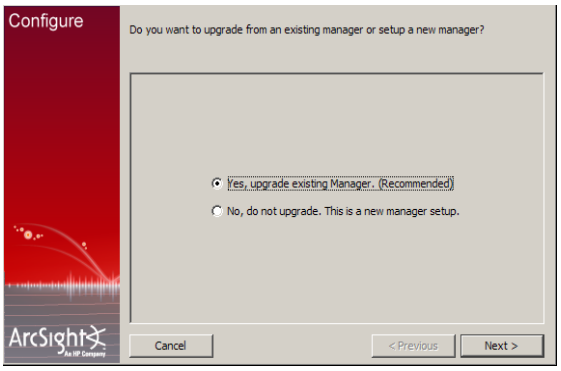

Do NOT install v5.2 Manager in the same location as the existing Manager.

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 `arcsight upgrade manager` command from the v5.2 Manager's `\bin` directory in the same command window where you had set the manager's heap size in Step d on page 22.

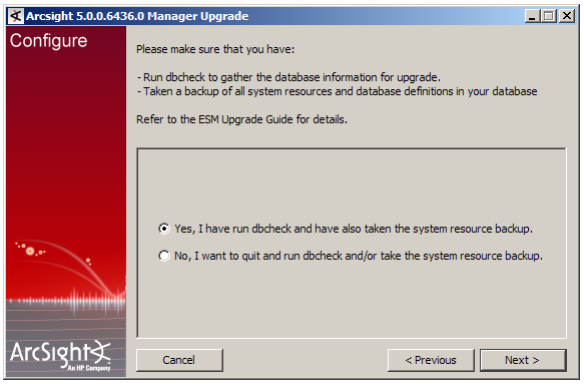
6 Select **Yes, upgrade existing Manager. (Recommended)**, and click **Next**.




7 You will see 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, 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.



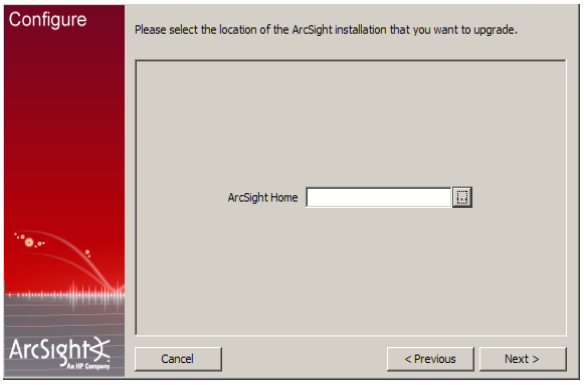

After you have run the `dbcheck` script, you can resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:

```
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.

9 Select the location of v5.0 SP1 or v5.0 SP2 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 20. Then go back to wizard and continue to completion.

10 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, a warning is generated.


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

Resolve duplicate names manually. Please contact Customer Support using the HP SSO website 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 v5.2 ArcSight Database installation's `ARCSIGHT_HOME/utilities/database/oracle/common/sql` directory 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 Customer Support using the HP SSO website.

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

12. You will see a message saying that you have completed the first stage of upgrade. 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 v5.0 SP1 or v5.0 SP2 system tables you exported in "Preparing the ArcSight Manager" on page 19 and then rerun:

`arcsight upgrade manager`

from the `/bin` directory of the location where you installed the v5.2 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 takes place:

- Upgrade system tables to v5.2
- Upgrade system indexes to v5.2
- Remove undelivered notifications
- Upgrade user functions

ArcSight's content is installed as follows:


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

- System Core content

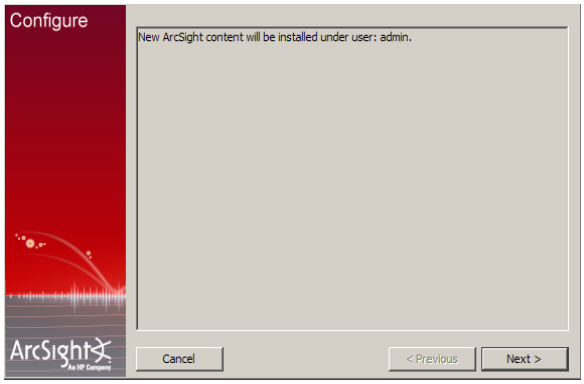
The System Core content provides the foundation building blocks for ArcSight ESM to work. This content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in `/All Filters/ArcSight System/Core`.

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.

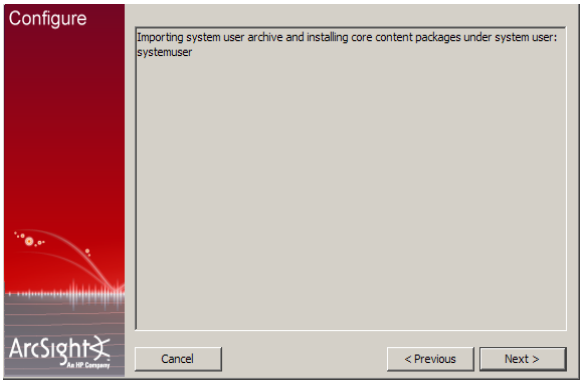
13 You will be informed that the ArcSight Content packages will be installed under user admin. This is the user that will own the system content. Click **Next**:




The following takes place:

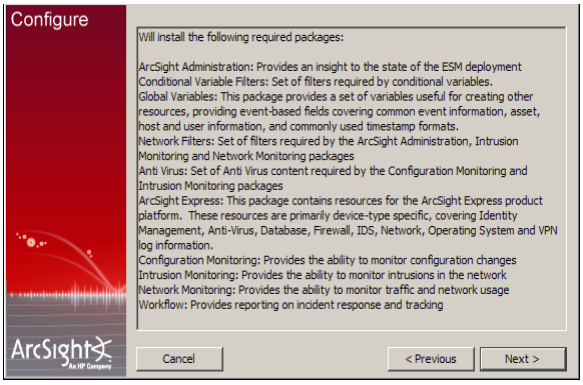
- Set enough cache size for resources
- Upgrade ArcSight system content resources

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



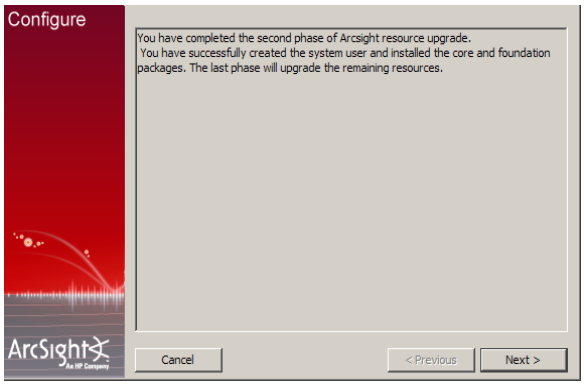

At this point the system user is updated and the core content is installed.

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




Click **Next**.

16 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

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

- Does a resource have valid values assigned to it?

  For example, the validation process checks if an IP address assigned to an asset falls in the range of IP address assigned to the zone to which the asset belongs. If the IP address is outside the range, this discrepancy is listed in a report that is generated at the end of the upgrade process.

- Does the resource satisfy its referential integrity?

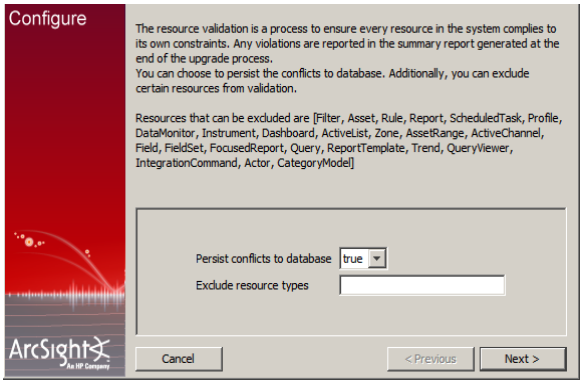
  For example, a rule depends on filters A, B, and C. If any of these filters is missing, the validation process will detect it and report it at the end of the upgrade process.

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

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

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

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





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

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

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

You need to have the same ARCSIGHT_JVM_OPTIONS as your v5.0 SP1 or v5.0 SP2 Manager when running this. See Step d on page 22 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, you need to update stats on the database by running the following command from the Database's `ARCSIGHT_HOME/bin`:

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

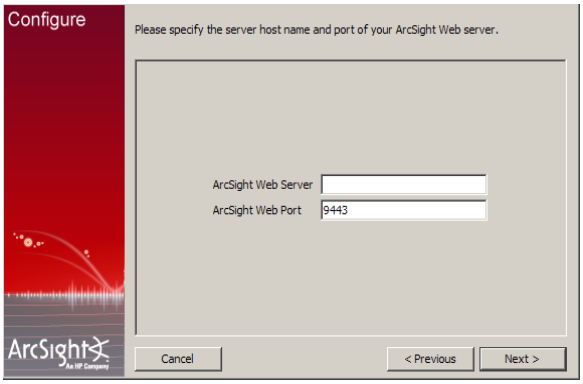
Click **Next**.

18 If you had an ArcSight Web server set up for your v5.0 SP1 or v5.0 SP2 installation or you want to set up an ArcSight Web server for v5.2, 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 SP1 or v5.0 SP2 and do not want to set up one for v5.2, select **Do not enter URL for ArcSight Web** and click **Next**.

19 If you are setting up an ArcSight Web server for v5.2, 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.)




20 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.

21 On Unix platforms, if you get a message saying changes to the service configuration require root privileges, follow the steps listed in the message.

22 During the upgrade, the v5.0 SP1 or v5.0 SP2 `config/server/agentURLMapping.csv` file is saved with the file extension `.previous` in the `config/server` directory of v5.2 `ARCSIGHT_HOME`. If you customized this file in v5.0 SP1 or v5.0 SP2 and want to use it for v5.2, rename the saved file to remove the `.previous` extension. That is, rename `agentURLMapping.csv.previous` to `agentURLMapping.csv`.

23 On successful completion of the upgrade, you will see a message to that effect. Click **Finish**.

24 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 SP1 or v5.0 SP2 to the v5.2 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.

25 Click **Done** in the last screen to exit the wizard.

You have upgraded ArcSight Manager to v5.2.


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.

# Post-Upgrade Tasks

You are required to do the following after upgrading your Manager to v5.2:

- 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 SP1 or v5.0 SP2 Manager when running this. See Step d on page 22 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 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 SP1 or v5.0 SP2 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.


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.

- 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 such processes manually.

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

# 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. 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 will be 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 Solaris, AIX, and Linux**:

     Run the following command:

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

     
     Note

     `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 archive is archived as expected.

Chapter 4

# Upgrading ArcSight Console

## Upgrading ArcSight Console

This upgrade process should be performed on all ArcSight Console instances that connect to the upgraded ESM v5.2 Manager.

The following platforms are supported for ArcSight Console:

| Platform | Supported Operating System | Typical System Requirements |
|---|---|---|
| Linux | Red Hat Enterprise Linux (RHEL) 5.7 Desktop 32-bit<br>Red Hat Enterprise Linux (RHEL) 6.1 64-bit | x86-compatible multi-CPU system with 2-4 GB RAM |
| Windows | Microsoft Windows Server 2003 R2 (SP2) 32 -bit<br>Microsoft Windows Server 2003 R2 (SP2) 64-bit<br>Microsoft Windows Server 2008 SP2 64-bit<br>Microsoft Windows 7 64-bit<br>Microsoft Windows 7 SP1 64-bit<br>Microsoft Windows Vista SP2 64-bit<br>Microsoft Windows Vista SP2 32-bit<br>Microsoft Windows XP Professional SP3 32-bit | x86-compatible single or multi-CPU system with 1-2 GB RAM |
| Macintosh OS X | Macintosh OS X 10.8 64-bit | |


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


**On Macintosh platform 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 v5.2 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-5.2.0.xxxx.0-Console-Win.exe`

   - **On Macintosh:**

     Run the following command.

     ```
     ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Console-MacOSX.zip -i console
     ```

   - **On Linux**:

     Run the following command.

     ```
     ./ArcSight-5.2.0.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-5.2.0.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 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 then click **Next**.
   - **Special Notice**—Read the notice and click **Next**.

- **Choose Installation Folder**—Enter an <ARCSIGHT_HOME> path for v5.2 that is different from where the existing Console is installed.

Note

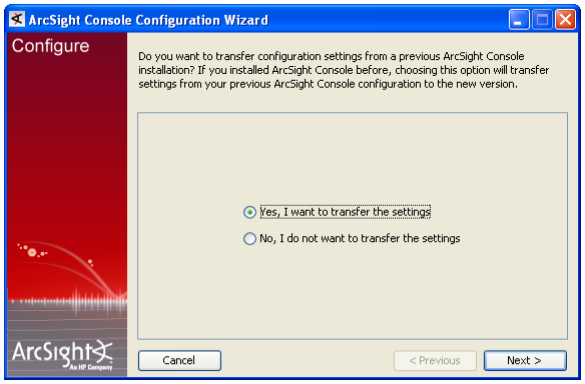
Do NOT install v5.2 Console in the same location as the existing Console.

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

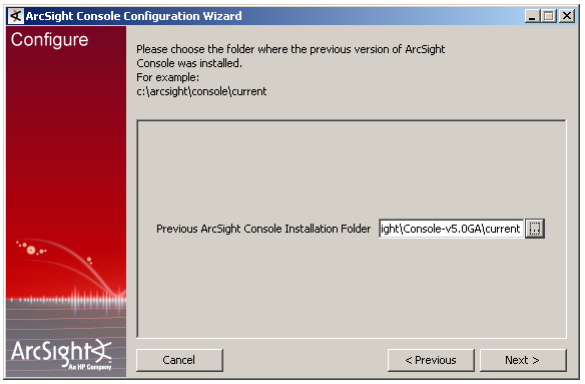
- **Choose Shortcut Folder** (on Windows) or **Choose Link Folder** (on UNIX)—Specify or select where the ArcSight Console icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows. Click **Next**.
- **Pre-Installation Summary—**Review the settings and click **Install**.

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

4 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.**




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




Note

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

Click **Next**.

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

7 Start the ArcSight Console.

A What's new Quick Start screen is displayed automatically. This screen summarizes the new features in ESM v5.2.

8 After you have upgraded a Console to v5.2:

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 the Customer Support using the HP SSO website.

Chapter 5

# Upgrading ArcSight Web

## Upgrading ArcSight Web

> **Note** The list of supported platforms for ArcSight Web v5.2 is same as the one for ArcSight Manager v5.2.

The following web browsers are supported in this release:

| Platform | Supported Browsers |
|---|---|
| Solaris SPARC | None |
| Windows | Internet Explorer 8.0, 9.0<br>Firefox 3.6, 5.0 |
| Linux | Firefox 3.6, 5.0 |
| Macintosh OS X | Safari 5.0,<br>Firefox 3.6, 5.0 |

Perform the following steps to upgrade your ArcSight Web.

1. Make sure that your Manager is up and running.
2. Stop ArcSight Web if it is running.
3. If you downloaded the compressed v5.2 ArcSight Web installation file to a different machine, transfer it to your ArcSight Web machine.
4. Extract the installation files from the compressed `ArcSight-5.2.x.nnnn.y-Web-<platform>.zip` file.

> **Note** Upgrading ArcSight Manager also requires you to extract its installation files from a compressed file. Installation files for ArcSight Web and ArcSight Manager should be **not** be present in the same folder. So, make sure that you do **not** extract the ArcSight Web files into the folder where you have extracted the ArcSight Manager files.

5. Start the installation as appropriate for your platform:
   - **On Windows**:

     Double-click `ArcSight-5.2.0.xxxx.0-Web-Win.exe`

- **On Solaris**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Web-Solaris.bin -i console
  ```

- **On AIX**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Web-AIX.bin -i console
  ```

- **On Linux**:

  Run the following command.

  ```
  ./ArcSight-5.2.0.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-5.2.0.xxxx.0-Web-Linux.bin -i console
  ```

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

- **Installation Process Checklist**—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 v5.2 that is different from where the existing Web is installed.


Do NOT install v5.2 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**.

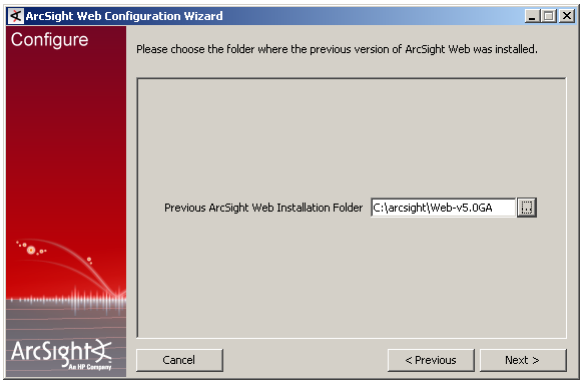
After you have stepped through the Installation wizard, it automatically starts the Configuration wizard.

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

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


Click **Next**.

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

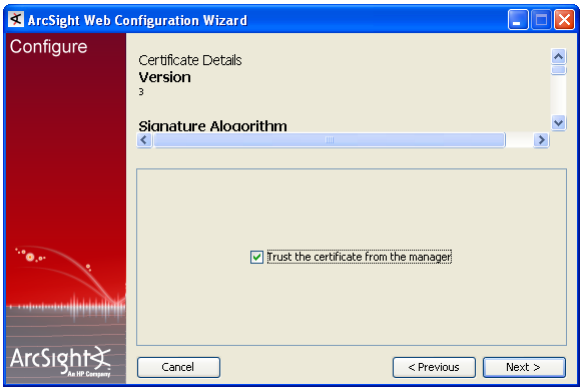



Navigate or enter the location for the previous ArcSight Web installation and click **Next**.

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**.

8 Follow the prompts in the next few screens.

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




10 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.

11 Start ArcSight Web.

Chapter 6

# 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 v5.2 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 SP1 or v5.0 SP2 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 v5.2. This may happen for assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In v5.2, 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 v5.2. 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 SP1 or v5.0 SP2 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 v5.2 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 v5.0 SP1 to v5.0 SP2 and are now upgrading to v5.2), 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 v5.2, 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 v3.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 v5.2 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 v3.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.


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.


Deprecated resources are no longer supported by ArcSight, so if you choose to restore a deprecated resource, you are responsible for its maintenance.

ArcSight also recommends that you verify whether the new v5.2 resources address the same goal more efficiently.

After v5.2 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. Enter the keyword "deprecated" in the **Search Query** field and click **Find**.

Chapter 7

# 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 v5.2 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 Hierarchical or Other Multi-Manager ArcSight™ ESM Installations to v5.2

This chapter describes the method for upgrading a multi-Manager deployment from v5.0 SP1 or v5.0 SP2 to v5.2.

## Summary

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

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

The process of upgrading ArcSight 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 ArcSight 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 ArcSight Manager.

1. First Upgrade any SmartConnectors that are not running a recent version. For best results use version 4.8.1 or later.
2. Stop your current ArcSight Manager.
3. Follow instructions in the Upgrading ArcSight ESM guide to upgrade your ArcSight Database software to v5.2.
4. Follow instructions in the Upgrading ArcSight ESM guide to upgrade your ArcSight Manager to v5.2.

5 Start the v5.2 Manager.

6 After the v5.2 Manager is running, follow instructions in the Upgrading ArcSight ESM guide to upgrade any Consoles connected to it.

7 Upgrade the **Forwarding Connector** connected to this manager to build `ArcSight-5.1.5.5973.0-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 Deploying ArcSight ESM for High Availability technical note 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 Arcsight 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