

Upgrading ArcSight™ ESM

v4.0 SP3 to v5.0 GA

June 14, 2010



Upgrading ArcSight™ ESM v4.0 SP3 to v5.0 GA

Copyright © 2010 ArcSight, Inc. All rights reserved.

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

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

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
06/14/10	Upgrading ArcSight ESM	v4.0 SP3 to v5.0 GA

Document template version: 1.0.2.7

ArcSight Customer Support

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

Contents

Chapter 1: Preparing for Upgrade	1
Document Status	1
Summary	1
Downloading installation files, scripts, and other documents	2
Chapter 2: Upgrading ArcSight Database	5
Preparing the ArcSight Database	5
Upgrading the ArcSight Database Software, Oracle, and Partition Archiver	7
Transferring Partition Archiver Settings	9
Chapter 3: Upgrading ArcSight Manager	13
Preparing the ArcSight Manager	13
Upgrading the ArcSight Manager	16
Post-Upgrade Tasks	24
Upgrading the Index	25
Updating and Starting the Partition Archiver Service	26
Chapter 4: Upgrading ArcSight Consoles	27
Upgrading ArcSight Consoles	27
Chapter 5: Upgrading ArcSight Web	31
Upgrading ArcSight Web	31
Chapter 6: Upgrading ArcSight SmartConnectors	35
Chapter 7: Checking the State of Existing Content After Upgrade	37
Index	45

Chapter 1

Preparing for Upgrade

Document Status

This technical note describes the steps required to upgrade the ArcSight ESM from v4.0 SP3 to v5.0 GA.



Caution

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

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

Summary

Upgrading ArcSight ESM involves the following steps:

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

[Upgrading ArcSight SmartConnectors](#)

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

[Upgrading ArcSight Manager](#)

[Upgrading ArcSight Consoles](#)

[Upgrading ArcSight Web](#)

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



Tip

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



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

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



ESM v5.0 GA does not support Oracle 10.2.0.2. If you are currently using Oracle 10.2.0.2, upgrade to Oracle 10.2.0.4 **before** you upgrade the ESM components. You will not be able to start ArcSight Manager if you have not upgraded to Oracle 10.2.0.4.

Downloading installation files, scripts, and other documents

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

You can do one of the following:

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

For the SmartConnectors:

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

For the Database:

- 1 Check the current ArcSight Database version you are running on the database machine. To check the version, in a v4.0 SP3 Console, click **Help | About**. The current version is displayed in 4.0.3.XXXX.n format, where XXXX is the build number and n is the patch number.
- 2 Download the database installation file appropriate for your platform. The following installation files are available:
 - ◆ `ArcSight-5.0.0.xxxx.0-DB-Win.exe`
 - ◆ `ArcSight-5.0.0.xxxx.0-DB-AIX.bin`
 - ◆ `ArcSight-5.0.0.xxxx.0-DB-Linux.bin`
 - ◆ `ArcSight-5.0.0.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 v4.0 SP3 Console that connects to the Manager, click **Help | About**. The current version is displayed in 4.0.3.XXXX.n format, where XXXX is the build number and n is the patch number.
- 2 Download the Manager installation file, as appropriate for your platform. These installation files are available:

- ◆ ArcSight-5.0.0.xxxx.0-Manager-Win.exe
- ◆ ArcSight-5.0.0.xxxx.0-Manager-Win64.exe
- ◆ ArcSight-5.0.0.xxxx.0-Manager-AIX.bin
- ◆ ArcSight-5.0.0.xxxx.0-Manager-Linux.bin
- ◆ ArcSight-5.0.0.xxxx.0-Manager-Linux64.bin
- ◆ ArcSight-5.0.0.xxxx.0-Manager-Solaris.bin

For the Consoles:

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

- ◆ ArcSight-5.0.0.xxxx.0-Console-Win.exe
- ◆ ArcSight-5.0.0.xxxx.0-Console-Linux.bin
- ◆ ArcSight-5.0.0.xxxx.0-Console-MacOSX.bin
- ◆ ArcSight-5.0.0.xxxx.0-Console-Solaris.bin

For ArcSight Web:

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

- ◆ ArcSight-5.0.0.xxxx.0-Web-Win.exe
- ◆ ArcSight-5.0.0.xxxx.0-Web-AIX.bin
- ◆ ArcSight-5.0.0.xxxx.0-Web-Linux.bin
- ◆ ArcSight-5.0.0.xxxx.0-Web-Solaris.bin

Other Documentation:

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

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

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



Note

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

Upgrading ArcSight Database

Preparing the ArcSight Database

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



Caution

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

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

Operating System	Database	Typical System Configuration
Microsoft Windows Server 2003 R2 (SP2) 32-bit Microsoft Windows Server 2003 R2 (SP2) 64-bit	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Red Hat Enterprise Linux 4.0 AS 32-bit update 8 Red Hat Enterprise Linux 4.0 AS 64-bit update 8 Red Hat Enterprise Linux 5 AS 32-bit Red Hat Enterprise Linux 5 AS 64-bit SUSE Linux 10 SP2 Enterprise Server 64-bit	Oracle 10.2.0.4	x86-compatible multi-CPU system with 2-16 GB RAM
Sun Solaris 10, 64-bit Ultra SPARC	Oracle 10.2.0.4	Sparc-compatible multi-CPU system with 2-16 GB RAM
IBM AIX 5L, Version 5.3 (5.3.0.70) 64-bit pSeries	Oracle 10.2.0.4	pSeries system with 2-16 GB RAM



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

- 2 If you downloaded the latest patch for your ArcSight Database, install it.

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

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

- a Shut down your v4.0 SP3 ArcSight Manager.

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

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

```
arcsight dbcheck
```

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

- `DatabaseInfo.htm`—Provides basic database information
- `EventIndexInfo.htm`
- `TablespaceInfo.htm`—Provides information such as free space, names of tablespaces, and so on
- `TableStatsInfo.htm`
- `PartitionInfoV40.htm`—Provides information about partitions
- `PartitionStatsInfo.htm`
- `ResourceCountV40.htm`—Provides resource count information

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

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

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

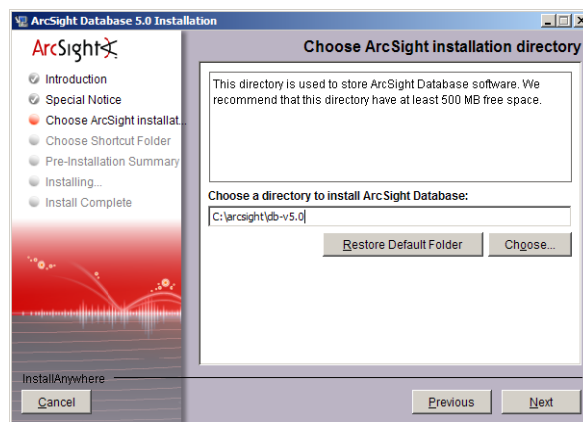
Upgrading the ArcSight Database Software, Oracle, and Partition Archiver



Caution

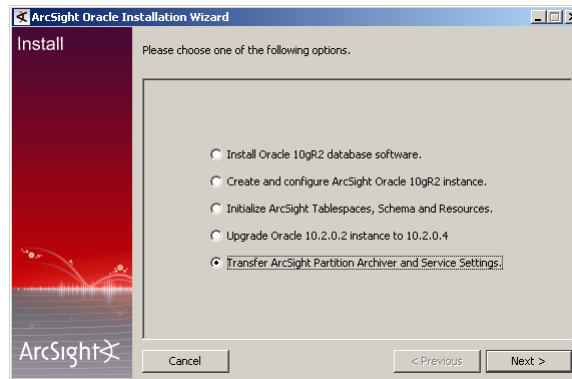
- Even if you choose to use your preexisting Oracle 10.2.0.4 installation, you must upgrade your ArcSight database software to v5.0 GA.
- ESM v5.0 GA does not support Oracle 10.2.0.2. If you are currently using Oracle 10.2.0.2, upgrade to Oracle 10.2.0.4 **before** you upgrade the Manager. You will not be able to start ArcSight Manager if you have not upgraded to Oracle 10.2.0.4.

- 1 Make sure to close any open connections to Oracle database before proceeding further.
- 2 If you downloaded the v5.0 GA ArcSight Database installation file on a different machine, transfer it to your Database machine.
- 3 If you have Partition Archiver service running on your v4.0 SP3 database machine, shut it down.
- 4 Log in as "root" on Unix and "Administrator" on Windows on the database server.
- 5 Run the database installation program.
- 6 Click **Next** in the Introduction and Special Notice screens.
- 7 Enter the location where you want to install the v5.0 GA database software. This location should be different from where you have the v4.0 SP3 database software installed.

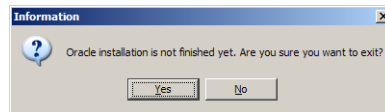


- 8 Click **Next**.
- 9 Step through the following screens:
 - ◆ **Choose Shortcut Folder** or **Choose Link Folder**—Specify or select where the ArcSight Database icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.
 - ◆ **Pre-Installation Summary**—Check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

- 10 Select an option in the following screen to suit your needs.



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



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



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

- ◆ If you have Partition Archiver configured in v4.0 SP3, you will need to transfer the Partition Archiver settings to your v5.0 GA 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 9](#) for details on the wizard screens that follow.



Notes about database upgrade

- The Partition Archiver service does not start automatically. Therefore, you must start the service manually once you have upgraded your Manager to v5.0 GA. See the section, ["Updating and Starting the Partition Archiver Service" on page 26](#) in the [Upgrading ArcSight Manager](#) chapter.
- If you have pre-v5.0 archived partitions and you had set up your Partition Archiver to archive with type uncompressed, backup your archive folder (that contains partition that you are trying to reactivate) before reactivation.

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

When Oracle Optimizer decides on a query execution plan, it can dynamically do a sampling of actual data to estimate the cost of the query. This will help improve query performance. To enable dynamic sampling, run the following commands while logged in as the oracle user (`su -oracle`):

```
% arcdbutil sql
Enter user-name: / as sysdba
```

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

Optional:

Run the following command while logged in as the oracle user (`su -oracle`) to update the IO transfer speed in the database. If you do not run this script, Oracle defaults to a very low IO transfer speed estimate that adversely affects the query execution plan.



Running the `SetDynamicSampling.sql` is not required if you had already upgraded your database to 10.2.0.4 with 4.0 SP3 release.

```
% arcdbutil sql
```

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

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

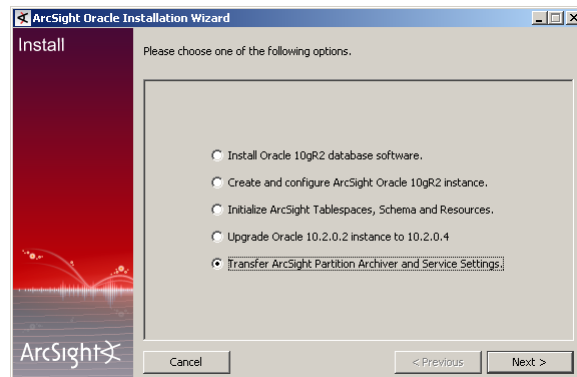


This script should be run every time you make any storage hardware changes that affects IO transfer speeds.

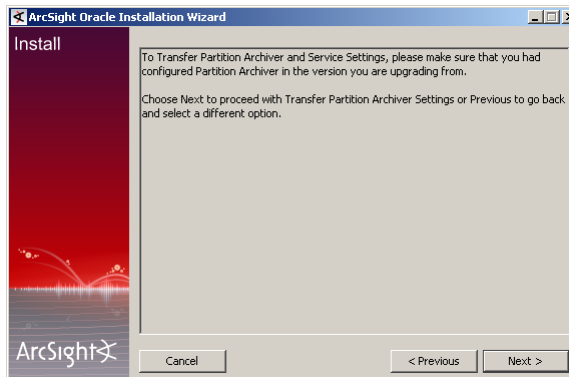
You have upgraded the ArcSight database v5.0 GA software. Go to the next section [Upgrading ArcSight Manager](#).

Transferring Partition Archiver Settings

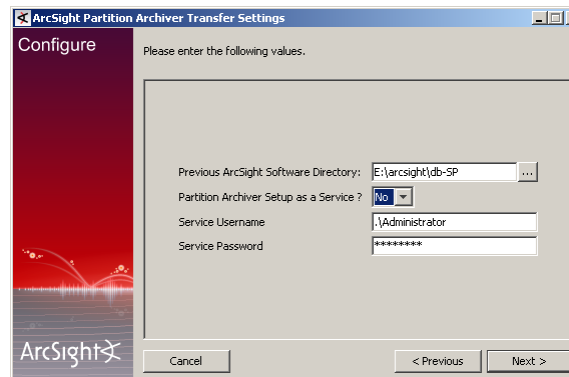
- 1 Select the **Transfer ArcSight Partition Archiver and Service Settings** option as shown and click **Next**:



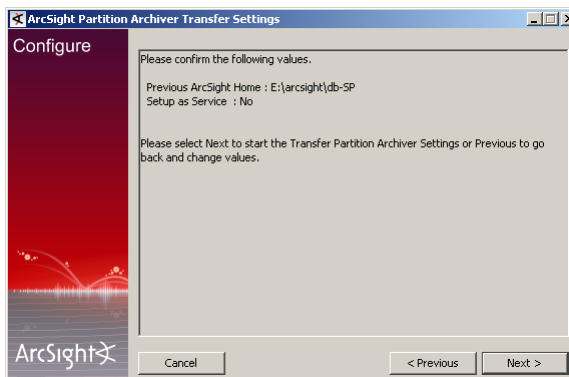
- 2 Click **Next** to confirm that you had configured the Partition Archiver in v4.0 SP3:



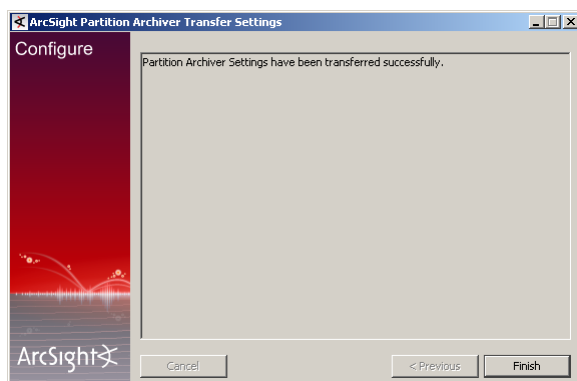
- 3 Enter the path name of the existing ArcSight Database's <ARCSIGHT_HOME> in the following screen and click **Next**:



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



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



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

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

Make sure to read the ["Notes about database upgrade" on page 8](#) and follow the instructions to enable dynamic sampling following it.

Chapter 3

Upgrading ArcSight Manager

Preparing the ArcSight Manager

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

Prepare ArcSight Manager as follows:

- 1 Verify that your database machine and version is supported for v5.0 from the list of supported platforms and database versions in ["Preparing the ArcSight Database" on page 5](#).
- 2 Verify that your Manager machine is supported for v5.0 from the list of supported platforms in the following table.



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

Platform	Supported Operating System	Typical System Requirements
Linux	Red Hat Enterprise Linux 4.0 (RHEL 4) AS 32-bit update 8	x86-compatible multi-CPU system with 2-4 GB RAM
	Red Hat Enterprise Linux 4.0 (RHEL 4) AS 64-bit update 8	
	Red Hat Enterprise Linux (RHEL 5) AS 32-bit	
	Red Hat Enterprise Linux (RHEL 5) AS 64-bit	
	SUSE Linux 10 SP2 Enterprise Server 64-bit	

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



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

- 3 If you downloaded the latest patch for your ArcSight Manager, install it.
- 4 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” on page 5. After running `dbcheck`, make sure that all log files the script generates are error and warning free.
- 6 Take a backup of all system resources and database definitions in your database. If the Manager upgrade process fails, you will need to restore your database to its original state before you can restart upgrade. This back up will be necessary in such a circumstance. Additionally, if you made changes to existing ArcSight-supplied resources, they will be overwritten during the upgrade. To restore your changes after the upgrade, you can use the backup copy as a reference.

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

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

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

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

PATH—Should be set to `$<ORACLE_HOME>/bin:$<PATH>` on UNIX and `%<ORACLE_HOME>%\bin;%<PATH>%` on Windows.
- c In `ARCSIGHT_HOME/bin` of your v4.0 SP3 database installation, run this command:

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

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

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

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

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



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

Upon successful completion, the command generates two files: a temporary parameter file and the actual database dump file called `arcsight.dmp`, which contains a dump image of the system tables. This file gets created in your v4.0 SP3 Database's `<ARCSIGHT_HOME>` directory.

- 7** By default, the heap size set for the upgrade process is 1 GB. If you have a large number of resources the upgrade process might need more memory. In such a situation, reset the heap size for the upgrade process to equal the heap size that you had set on your v4.0 SP3 Manager. To do so,

- a** Run the following command from your v4.0 SP3 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 v4.0 SP3 Manager.

On Windows:

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

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

On Unix:

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

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

Upgrading the ArcSight Manager



Do not upgrade ArcSight Manager until you have successfully upgraded ArcSight Database and successfully exported system tables as described in [“Preparing the ArcSight Manager” on page 13](#).



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

Perform these steps to upgrade your Manager:

- 1 If you downloaded the v5.0 GA Manager installation file to a different machine, transfer it to your Manager system.
- 2 Make sure that the Manager is stopped.

For instructions about shutting down your ArcSight Manager, see *ArcSight ESM Administrator's Guide*.
- 3 Log in as user “arcsight” on the Manager machine.

This step is required because the v5.0 GA Manager cannot be installed using the “root” user account for security reasons.
- 4 Run the installation command, as appropriate for your platform, from the directory where you downloaded the installation file.

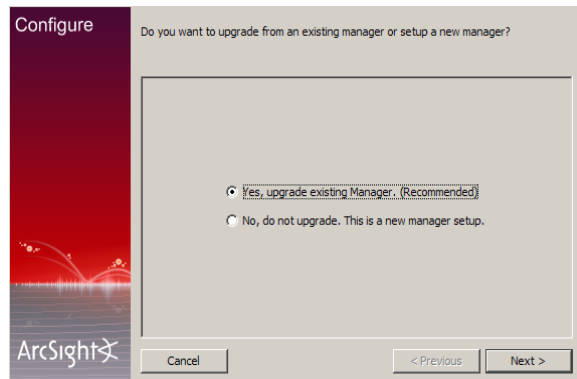
For example, run `./ArcSight-5.0.0.XXXX.0-Manager-Linux.bin` on a Linux machine or on Windows, double-click on the `ArcSight-5.0.0.XXXX.0-Manager-Win.exe` file.
- 5 Step through the Installation wizard screens. Specifically, enter values as described below for the following wizard screens:
 - ◆ **Choose ArcSight Installation Directory**—Enter an `<ARCSIGHT_HOME>` path for v5.0 GA that is different from where the existing Manager is installed. Click **Next**.



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

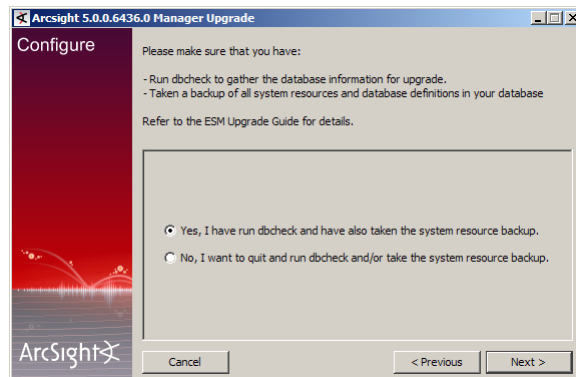
Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

- ◆ **Choose Shortcut Folder** (on Windows)/**Choose Link Folder** (on UNIX)—Specify or select where the ArcSight Manager icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows. Click **Next**.
 - ◆ **Pre-Installation Summary**—Review the settings and click **Install**.
- 6 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 v5.0 Manager's `\bin` directory in the same command window where you had set the manager's heap size.



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](#)” on page 5, you must run it and make sure that all log files the script generates are error and warning free. Also, you should have made a backup of the system dump by this point. If you have not done so yet, do that before continuing with the upgrade.
 - ◆ To stop the Manager upgrade at this point, select **No, I want to quit and run dbcheck** and click **Next** in the following screen.



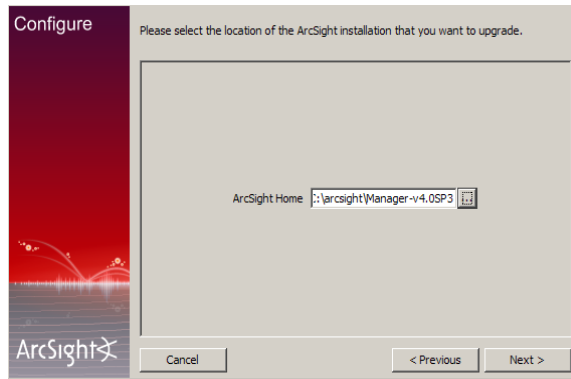
After you have run the `dbcheck` script, you can resume the Manager upgrade by running this command in `<ARCSIGHT_HOME>/bin`:

```
arcsight upgrade manager
```

The upgrade process resumes from this point.

- ◆ To continue with Manager upgrade, select **Yes, I have run dbcheck and the database is OK** and click **Next** in the above screen.

- 9 Select the location of v4.0 SP3 installation in the following screen and click **Next**:



- 10 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, you will receive a warning message telling you so. You are required to resolve such resources manually so that all resources in a group have unique names before proceeding further with the upgrade. Contact ArcSight Customer Support if you need assistance doing this.

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

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

- a Check for duplicate resource names. Enter these commands in the v5.0 GA ArcSight Database installation's `ARCSIGHT_HOME/utilities/database/oracle/common/sql` on your **database** machine to obtain a complete list of duplicate resource names:

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

```
SQL> SET SERVEROUTPUT ON
```

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

This creates the `CheckDupNames.sql` procedure.

```
SQL> EXEC CHECKDUPNAMES
```

- b Resolve the duplicate names manually.

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

- 11 The upgrade process also checks for pre-v5.0 archived partitions with archive type uncompressed which are in reactivated state. If you have such partitions, deactivate them before you do the Manager upgrade.

- 12** You will see a screen informing you that you have completed the first stage of the Manager upgrade. Click **Next**.



Note

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

If you still get an error, import the v4.0 SP3 system tables you exported in [“Preparing the ArcSight Manager” on page 13](#) and then rerun:

```
arcsight upgrade manager
```

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

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

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

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

At this point the following takes place:

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

ArcSight's stock content is installed as follows:



Note

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

- ◆ System Core content

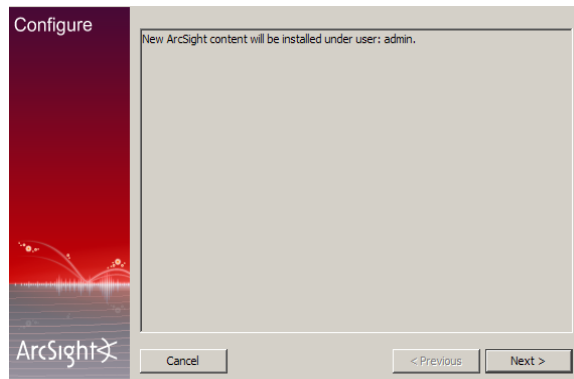
The System Core content provides the foundation building blocks for ArcSight ESM to work. This content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in `/All Filters/ArcSight System/Core`.

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

- ◆ Foundation content

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

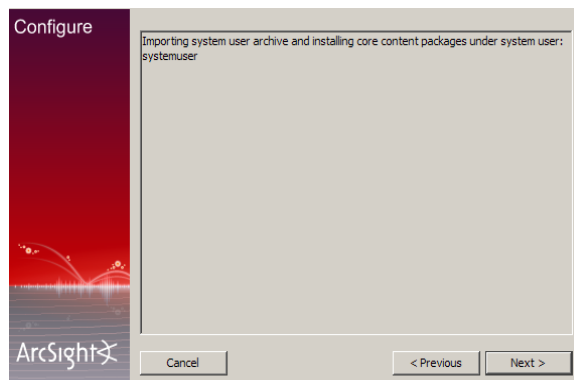
- 13** You will be informed that the ArcSight Content packages will be installed under user admin. This is the user that will own the system content. Click **Next**:



The following takes place:

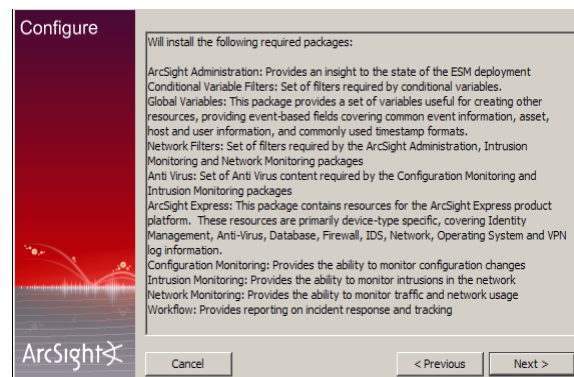
- ◆ Set enough cache size for resources
- ◆ Upgrade ArcSight system content resources

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



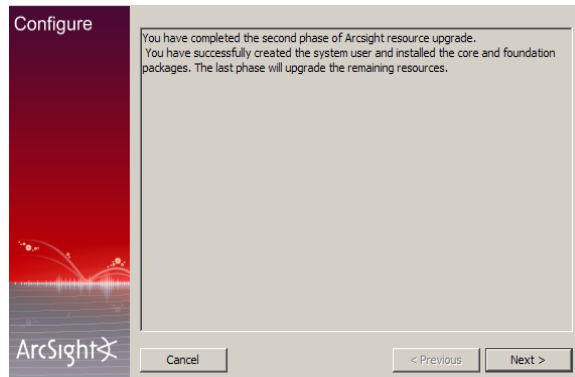
At this point the system user is updated and the core content is installed.

- 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:



Note

From this point in the upgrade process, you cannot roll back to the previous version of ESM.

If you go through all the subsequent screens in the wizard and the upgrade completes normally, your system is upgraded successfully and will be in a usable state.

If you run into any issues, rerun the upgrade program.

- If you see the following message:

```
Schema version 5.0.xxxx.0 is current. The ArcSight
installation is already updated to the latest version.
```

it is an indication that one or more of the post upgrade tasks (Preserve Case Events and/or Resource Validation Update) failed. Check the log files to find out which one may have failed and rerun it independently from the Manager's \bin directory after you have completed the upgrade:

If preserve case events failed, run:

```
arcsight preservecaseevent
```

If resource validation failed, run:

```
arcsight resvalidate -persist
```

You need to have the same ARCSIGHT_JVM_OPTIONS as your v4.0 SP3 Manager when running this. See [Step d on page 15](#) for details on setting ARCSIGHT_JVM_OPTIONS.

- If you see the following error:

```
A previous attempt to upgrade failed while updating event
tables. Please contact ArcSight support for help.
```

it is an indication that the event schema update failed. Contact ArcSight Customer Support to recover from the failure.

Click **Next**.

At this point the following happens:

- ◆ User's personal group upgrade
- ◆ Resource Fixup
- ◆ Viewer configuration upgrade
- ◆ Upgrade event tables to v5.0
- ◆ Create case event table indexes
- ◆ Update the database schema version to v5.0
- ◆ Preserve events in cases

- 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.

Configure

The resource validation is a process to ensure every resource in the system complies to its own constraints. Any violations are reported in the summary report generated at the end of the upgrade process. You can choose to persist the conflicts to database. Additionally, you can exclude certain resources from validation.

Resources that can be excluded are [Filter, Asset, Rule, Report, ScheduledTask, Profile, DataMonitor, Instrument, Dashboard, ActiveList, Zone, AssetRange, ActiveChannel, FocusedReport, Query, ReportTemplate, Trend, QueryViewer]

Persist conflicts to database:

Exclude resource types:

Cancel < Previous Next >



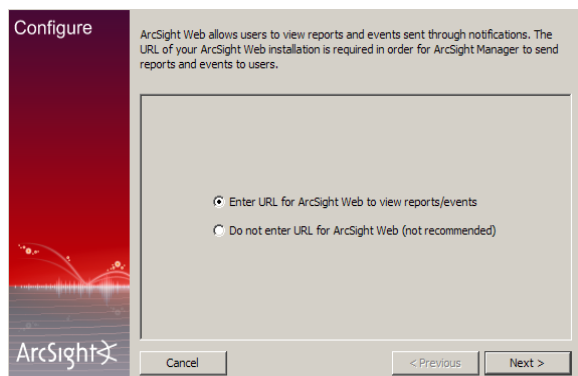
Tip

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

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

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

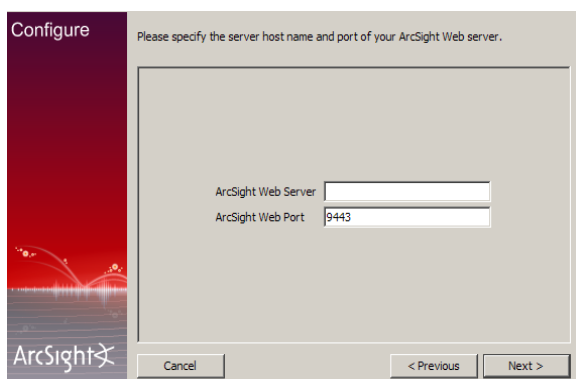
- 18** If you had an ArcSight Web server set up for your v4.0 SP3 installation or you want to set up an ArcSight Web server for v5.0 GA, select **Enter a URL for ArcSight Web to view report/events** and click **Next** in the following screen:



If you did not have an ArcSight Web server set up for v4.0 SP3 and do not want to set up one for v5.0 GA, select **Do not enter URL for ArcSight Web** and click **Next**.

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

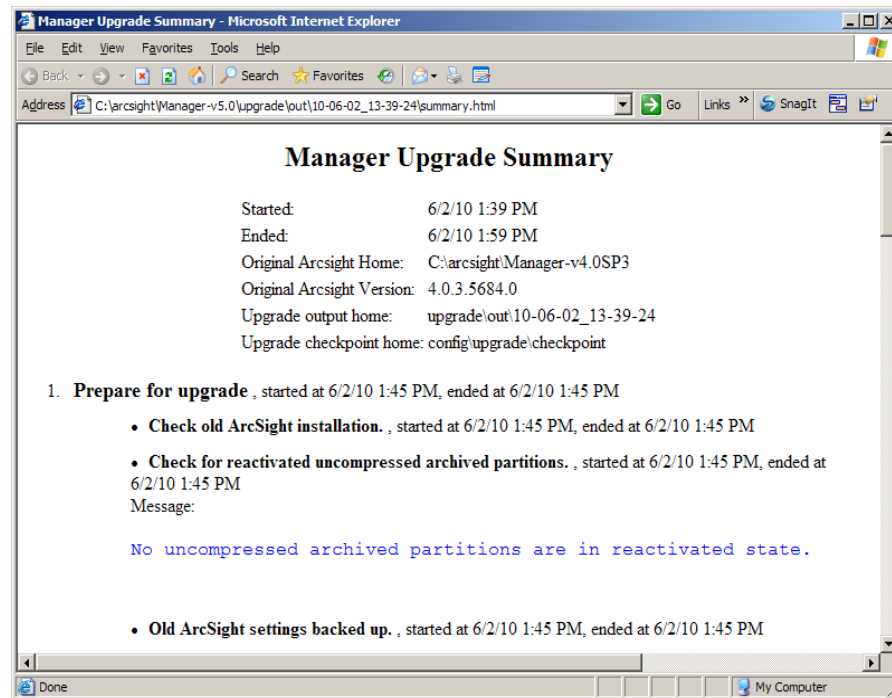


- 20** Select whether you want to install the Manager as a service. The option you select from these Manager startup options will take effect when the Manager machine reboots.
- 21** On Unix platforms, if you get a message saying changes to the service configuration require root privileges, follow the steps listed in the message.
- 22** During the upgrade, the v4.0 SP3 `config/server/agentURLMapping.csv` file is saved with the file extension `.previous` in the `config/server` directory of v5.0 GA `ARCSIGHT_HOME`. If you customized this file in v4.0 SP3 and want to use it for v5.0 GA, rename the saved file to remove the `.previous` extension. That is, rename `agentURLMapping.csv.previous` to `agentURLMapping.csv`.
- 23** You will see a message on successful completion of the upgrade.
- 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 v4.0 SP3 to the v5.0 GA installation or fixing invalid resources.

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

The following screen shows part of an example summary report:



On Unix machines, make sure that 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 v5.0 GA.

Post-Upgrade Tasks

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

- Starting with ESM v5.0, all events belonging to Cases are automatically preserved in the database. They are available as part of the Cases even beyond the online retention period of Events.

Case event preservation gets taken care of transparently during the upgrade process. But if you have a large number of cases, this process can take thirty minutes or longer. In such a situation, the upgrade process will time out and you will see a message saying so in the upgrade summary. If that happens, run the following from the Manager's `\bin` directory:

```
arcsight preservcaseevent
```

- 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 v4.0 SP3 Manager when running this. See [Step d on page 15](#) for details on setting ARCSIGHT_JVM_OPTIONS.

- If you plan to use the Domain Field Sets feature, you are required to upgrade your index to accommodate the changes in schema that affect the ARC_EVENT_INDEX table. See ["Upgrading the Index" on page 25](#) for details.
- You are required to manually run the following script to disable the oracle nightly stats that run over arcsight schema. Run the following commands while logged in as the oracle user (`su -oracle`):

```
% arcdbutil sql
```

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

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

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

```
arcsight refcheck -f true
```

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

- During upgrade, the "Default User Groups" user group is updated and adds the `/All Filters/ArcSight System/Core/No Events` filter to the events ACL. If the Forwarding Connector user is in that group, the connector cannot send events to the destination Manager. To prevent this problem, edit the access control for the Forwarding Connector's parent user group and select a filter that gives permission to the subset of events for which the user has access.

Alternatively, if the user has access to all the events, delete the `/All Filters/ArcSight System/Core/No Events` filter.

- File resources are not handled properly during ESM upgrading. This results in unassigned file resources after the upgrade. For example, `.art` files are created as new file resources in ESM v4.5 SP1 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.

You can now start the Manager.



Note

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

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

Upgrading the Index

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

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

- Amount of available space in the ARC_EVENT_INDEX tablespace

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

- Length of system downtime allocated for this upgrade

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

After the upgrade to v5.0 Manager is complete, run this command in `ARCSIGHT_HOME/bin` to start the Index Upgrade wizard:

```
arcsight upgrade index
```

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

Updating and Starting the Partition Archiver Service

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

- 1 Run the following command (on unix machines, logged in as user 'oracle') from the Database `bin` directory to update the Partition Archiver:

```
arcsight agentsetup -w
```

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

- ◆ **On Windows:**

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

- ◆ **On Solaris, AIX, and Linux:**

Run the following command:

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



`arc_oraclepartitionarchiver_db` is the default service name.

Note

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

Upgrading ArcSight Consoles

Upgrading ArcSight Consoles

The following platforms are supported for ArcSight Console:

Platform	Supported Operating System	Typical System Requirements
Linux	Red Hat Enterprise Linux 4.0 (RHEL 4) WS 32-bit Update 8	x86-compatible multi-CPU system with 2-4 GB RAM
	Red Hat Enterprise Linux 4.0 (RHEL 4) AS 64-bit Update 8	
	Red Hat Enterprise Linux (RHEL 5) 32-bit	
Solaris	Sun Solaris 10 (05/09) SPARC, 64-bit	Sparc-compatible multi-CPU system with 2-4 GB RAM
Windows	Microsoft Windows Server 2003 R2 (SP2) 32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM
	Microsoft Windows Server 2003 R2 (SP2) 64-bit	
	Microsoft Windows Server 2008 SP2 64-bit	
	Microsoft Windows Vista SP2 64-bit	
	Microsoft Windows Vista SP2 32-bit	
	Microsoft Windows XP Professional SP3 32-bit	
Macintosh OS X	Macintosh OS X 10.5.6 64-bit	



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

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

- 1 Stop ArcSight Console if it is running.
- 2 If you downloaded the v5.0 GA Console installation file to a different machine, transfer it to your Console machine.
- 3 Run the installation file.
- 4 Step through the Installation wizard screens. Specifically, enter values as described below for the following wizard screens:
 - ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v5.0 GA that is different from where the existing Console is installed. Click **Next**.

**Note**

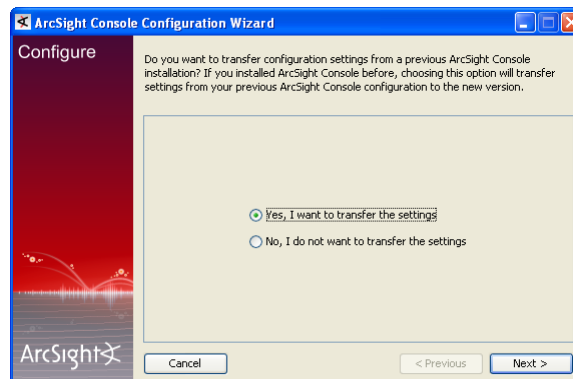
Do NOT install v5.0 GA Console in the same location as the existing Console.

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

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

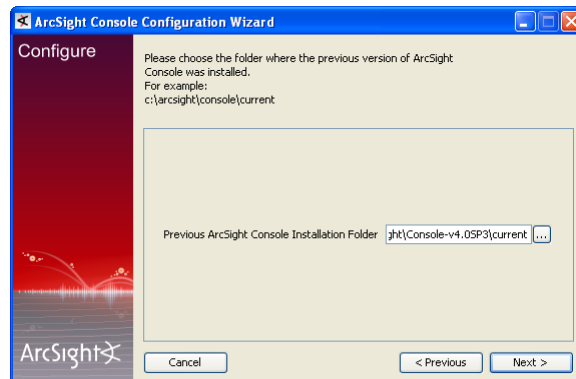
- 5 The Console installation program detects a previous installation and provides you an option to copy your existing settings to the new Console. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type. Select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



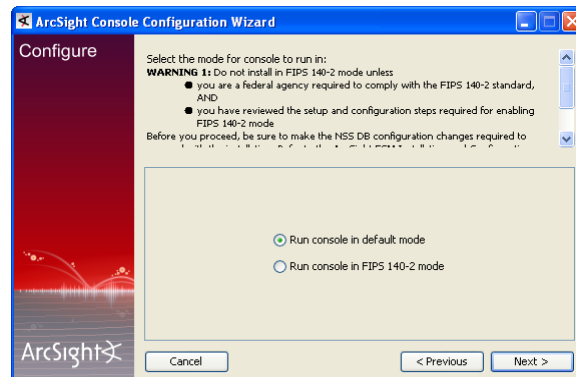
- 6 If you selected **Yes, I want to transfer the settings**, you will be prompted to enter the location of your previous Console installation:

**Note**

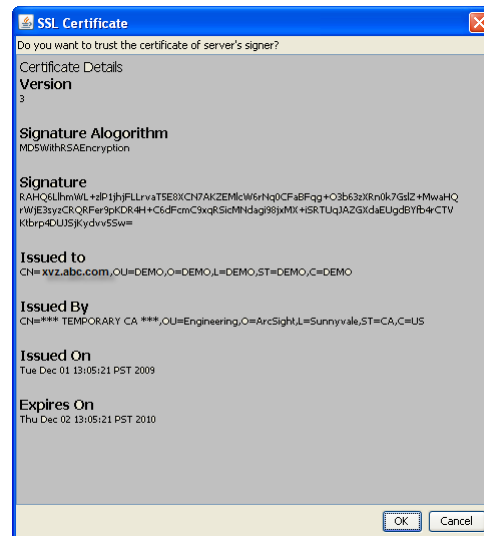
Be sure to select `<ARCSIGHT_HOME>\current` directory of your previous installation as shown in the screenshot below.



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



- 8** See the *ArcSight ESM Installation and Configuration Guide* for details on the remaining screens for installing a Console using the installation wizard.
- 9** Start the ArcSight Console. After you log in, you will see a dialog asking you whether you want to trust the Manager's certificate signer:



Click **OK** to accept the certificate.

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

10 After you have upgraded a Console to v5.0 GA, make sure:

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

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

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

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

Chapter 5

Upgrading ArcSight Web

Upgrading ArcSight Web



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

The following web browsers are supported in this release:

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

Perform the following steps to upgrade your ArcSight Web.

- 1 Make sure that your Manager is up and running.
- 2 Stop ArcSight Web if it is running.
- 3 If you downloaded the v5.0 GA ArcSight Web installation file to a different machine, transfer it to your ArcSight Web machine.
- 4 Run the installation file.
- 5 Step through the Installation Wizard screens. Specifically, enter values as described below for the following Wizard screens:
 - ◆ **Choose Installation Folder**—Enter an `<ARCSIGHT_HOME>` path for v5.0 GA that is different from where the existing Web is installed.



Do NOT install v5.0 GA Web in the same location as the existing Web. Installing in a different location prevents the installation program from overwriting your existing configuration, thus enabling you to migrate settings from it.

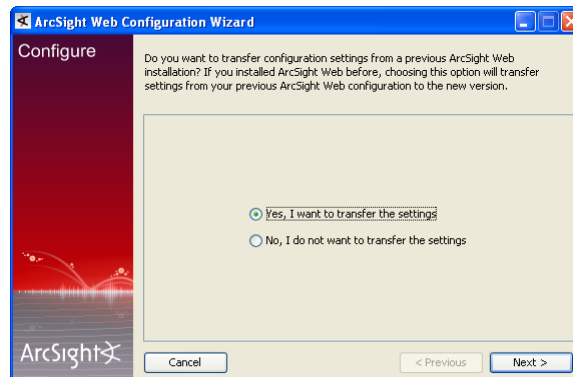
- ◆ **Choose Shortcut Folder** (on Windows)/**Choose Link Folder** (on UNIX)—Specify or select where the ArcSight Web icon will be created; for example, in an existing Program Files Group or on the Desktop on Windows.

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

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

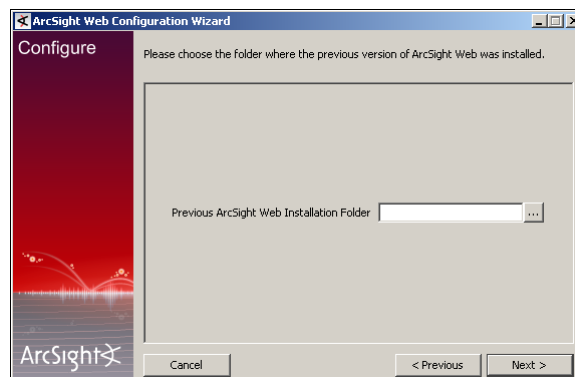
- 6 The Web installation program detects a previous installation and provides you an option to copy your existing settings to the new Web. Settings such as connection information including the Manager host name and port number, and authentication information including authentication type.

Copying existing settings is optional.



Click **Next**.

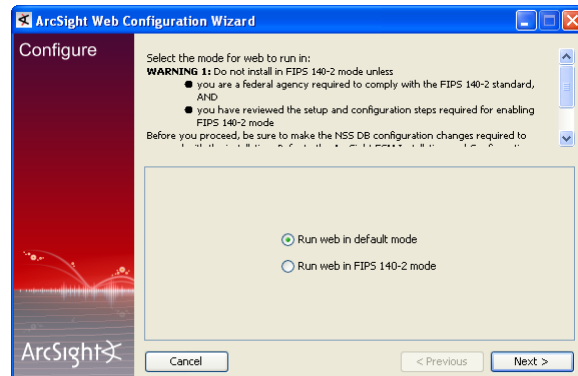
- 7 If you selected **Yes, I want to transfer the settings**, the Web installation program prompts you to enter the location for your previous installation.



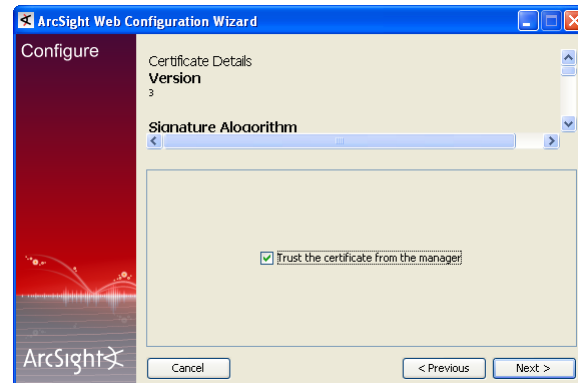
Navigate or enter the location for the previous ArcSight Web installation and click **Next**.

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



- 9** Follow the prompts in the next screens.
- 10** Make sure to check the box in the following screen in order to trust the Manager's certificate.



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

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

- 12** Start ArcSight Web.

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 release 4.0.1.4785.0 or above in order to avoid DST-related issues. Refer to the DST documents provided on the ArcSight Support download site for details.

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

Perform the following steps to upgrade SmartConnectors:

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

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

For an overview of the SmartConnector installation and configuration process, see the *SmartConnector User's Guide*. For complete installation instructions for a particular SmartConnector, see the configuration guide for that connector. The product-specific configuration guide provides specific device configuration information, installation parameters, and device event mappings to ArcSight ESM fields.

Checking the State of Existing Content After Upgrade

After the upgrade is complete, do the following checks to verify that all your content has been successfully transferred to the v5.0 GA structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

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

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

- **Restore customizations to resources with the original resource IDs.** If you had custom configurations to any resource with an original ArcSight resource ID, restore your configurations manually after upgrade is complete from the backed up version you saved before upgrade.
- **Assets Resource.** The Disabled group in the assets resource tree is dynamic, which means it queries the Manager every two minutes for assets that have been disabled. After upgrade, check to see if any assets were disabled and moved to the Disabled group in the Assets resource tree.
 - ◆ If so, review the disabled asset to see the reason it was disabled and fix it as appropriate. For example, if an asset's IP address is outside the range of the upgraded zone, either expand the range of the zone, or assign the asset to another zone.
 - ◆ You can also delete an asset that has become disabled if it is no longer needed (right-click the asset and select **Delete**).
- For existing assets, if two assets **in the same zone** have the same hostname or IP address one of them becomes invalid after the ESM upgrade to v5.0. This may happen for assets whose hostnames are Fully Qualified Domain Name (FQDN) of the asset. In v5.0, only the hostname 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 hostname is identical, these two assets are considered as conflicting assets and one of them becomes invalid.

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

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

- **Users Resource.** Only the system user has access privileges to the [/All Users](#) resource tree. Therefore, any users or groups you created in [/All Users](#) in the previous installation are now available under [Custom User Groups](#).

After upgrade, verify that your user ACLs are correct and still valid based on how ArcSight standard content is organized for v5.0 GA. For example, Administrator access should only be granted to those with authority to work with system-level content, such as ArcSight System and ArcSight Administration. Update user ACLs manually as appropriate.
- **Zones Resource.** Check to see if any zones were invalidated during the upgrade process.
 - ◆ Fix zones that may have become invalid during upgrade that you want to keep.
 - ◆ Verify that the assets assigned to zones that have been moved or invalidated during the upgrade retain their connections to the appropriate v4.0 SP3 zones.
 - ◆ Delete any invalid zones that you no longer want to keep.
 - ◆ If you made customizations to the standard v4.0 SP3 zones, manually edit the new resource to restore the customizations you made to the v4.0 SP3 zone. Do not import the old zone.
- **Repair any invalid resources.** During the upgrade process, the resource validator identifies any resources that are rendered invalid (conditions that no longer work) during the upgrade. Review the upgrade summary report in [ARCSIGHT_HOME/upgrade/out/<time_stamp>/summary.html](#) to find invalid resources and fix their conditions as appropriate.
- If you have upgraded your ESM installation more than once (for example, from v4.0 to v4.5, then v4.5 and are now upgrading to v5.0), 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).
- This bullet item applies to you only if you are upgrading from v3.5 SP2 all the way to v5.0 GA (that is, if your ESM was upgraded from v3.5 SP2 to v4.0 SP1, and later upgraded to v4.0 SP3, then v4.5 SP1, and lastly to v5.0 GA.)

The data type used for case stage has been updated to be of enumeration data type instead of the String data type used in previous ESM releases. So, if you had Case queries in your system that used string operators on the Case Stage field (for example "stage startsWith 'F'"), you will be required to manually fix those conditions to use operators valid on enumeration data types. For example, if you have a condition "stage startsWith 'F'" and there are two possible enumeration values (2, Final) and (5, Follow-up), you should change the condition to "stage = Final or stage = Follow-up".
- **Verify that customer-created content still works as expected.** Customer-created content that refers to ArcSight standard content and has been significantly changed may not work as expected.

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

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

 - ◆ Send events that you know should trigger the content through the system using the Replay with Rules feature. For more information about this feature and how

it's been enhanced for v5.0 GA, 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.
- In v5.0, some zones were renamed, merged, or split. This means that some of the zones changed when you upgraded to v5.0 depending on whether they were merged, split, or renamed. This redefinition of zones can have an impact on other resources too, such as assets, asset ranges, active and session lists, etc.

How individual Assets are handled after upgrade:

ESM v5.0 introduces the auto-zoning feature for assets. An example of the auto-zoning feature is as follows: Say Asset 1 with an IP address of 3.0.0.1 used to belong to Zone A (Zone A 1.0.0.0 - 3.255.255.255) and Zone A was split as follows:

Zone A' 1.0.0.0 - 1.255.255.255

Zone B 2.0.0.0 - 2.255.255.255

Zone C 3.0.0.0 - 3.255.255.255

After upgrade, Asset 1 will automatically be put in Zone C, because according to the new zoning definition, its IP address is now in the Zone C range.

How Asset Ranges are handled after upgrade:

In v4.0 or v4.5, if you had an asset range in Zone A, the asset range might become invalid after the upgrade to v5.0 if Zone A was split and if your asset range now spans over two zones. For example, suppose Zone A was split into two zones, Zone A and Zone B, and after upgrade your asset range spans over the last part of Zone A and first part of Zone B, your asset range will become invalid. You need to open the invalid asset range resource, and map it to the right zone, or split it into 2 asset ranges that map to the new zones A and B.

How Assets in Active List and Session Lists are handled after upgrade:

If an active list or session list has upgraded zone resource references in it, you might need to update them too, otherwise a rule having an InActiveList condition on the pre-updated zones will not trigger. If there are several hundred entries, unless you have manually populated these entries, it is best to let the rules that maintain the lists continue to do so. Active lists entries may require removing the old entries and re-entering them with the updated zone information. Session list entries may not require removing the session information for the old data, but terminating the entry before entering the updated information may be required.

How Trends are handled after upgrade:

Trends often use zone resource references, rather than zone names, when collecting their information. This makes writing queries on such trends easier, because all the information regarding the zone, e.g., zone URI, zone name, etc., is available via the zone resource reference. The drawback to this is that the zone upgrade process might change to which zone a zone resource reference may refer. This may affect the way assets appear in a report using that trend.

For example, let us assume that there is an asset, Asset A, which falls under Zone A before the upgrade. Also assume that after the upgrade two things happen:

- ◆ Asset A now falls under Zone B
- ◆ Zone A gets renamed to Zone C.

If a trend collects data on Asset A every day for a week (Sunday - Saturday) and the upgrade is done on Wednesday you might expect the following:

Date	Asset	Zone Name
Sun	Asset A	Zone A
Mon	Asset A	Zone A
Tue	Asset A	Zone A
Wed	Asset A	Zone A
Thu	Asset A	Zone B
Fri	Asset A	Zone B
Sat	Asset A	Zone B

But, instead, you will see this:

Date	Asset	Zone Name
Sun	Asset A	Zone C
Mon	Asset A	Zone C
Tue	Asset A	Zone C
Wed	Asset A	Zone C
Thu	Asset A	Zone B
Fri	Asset A	Zone B
Sat	Asset A	Zone B

Such reports may appear this way until the time range covered by the trend starts after the date of the upgrade. It is not possible to update the trend entries like the active or session lists.

List of zones that were changed in v5.0:

The following table lists the zones that have been split, merged or renamed in ESM v5.0:

4.x Zones		5.0 Zones	
Group	Zone Name	Group	Zone Name
Dark Address	1.0.0.0-2.255.255.255 (IANA)	Public	1.0.0.0-1.255.255.255 (APNIC)
			2.0.0.0-2.255.255.255 (RIPE NCC)
Dark Address	100.0.0.0-111.255.255.255 (IANA)	Dark Address	100.0.0.0-107.255.255.255 (IANA)
Public	112.0.0.0-126.255.255.255 (APNIC)	Public	110.0.0.0-126.255.255.255 (APNIC)

4.x Zones		5.0 Zones	
Public	128.0.0.0-169.253.255.255	Public	128.0.0.0-140.255.255.255 (ARIN)
			141.0.0.0-141.255.255.255 (RIPE NCC)
			142.0.0.0-144.255.255.255 (ARIN)
			145.0.0.0-145.255.255.255 (RIPE NCC)
			146.0.0.0-149.255.255.255 (ARIN)
			150.0.0.0-151.255.255.255 (APNIC)
			152.0.0.0-152.255.255.255 (ARIN)
			153.0.0.0-153.255.255.255 (APNIC)
			154.0.0.0-154.255.255.255 (AfrinIC)
			155.0.0.0-162.255.255.255 (ARIN)
			163.0.0.0-163.255.255.255 (APNIC)
			164.0.0.0-169.253.255.255 (ARIN)
Public	169.255.0.0-172.15.255.255	Public	169.255.0.0-170.255.255.255 (ARIN)
			171.0.0.0-171.255.255.255 (APNIC)
			172.0.0.0-172.15.255.255 (ARIN)

4.x Zones		5.0 Zones	
Dark Address	175.0.0.0-185.255.255.255 (IANA)	Public	175.0.0.0-175.255.255.255 (APNIC)
		Dark Address	176.0.0.0-177.255.255.255 (IANA)
		Public	178.0.0.0-178.255.255.255 (RIPE NCC)
		Dark Address	179.0.0.0-179.255.255.255 (IANA)
		Public	180.0.0.0-180.255.255.255 (APNIC)
		Dark Address	181.0.0.0-181.255.255.255 (IANA)
		Public	182.0.0.0-183.255.255.255 (APNIC)
			184.0.0.0-184.255.255.255 (ARIN)
		Dark Address	185.0.0.0-185.255.255.255 (IANA)
Public	186.0.0.0-192.0.1.255	Public	186.0.0.0-187.0.0.0 (LACNIC)
			188.0.0.0-188.255.255.255 (RIPE NCC)
			189.0.0.0-191.255.255.255 (LACNIC)
			RFC5736: IANA IPv4 Special Purpose Address Registry (192.0.0.0-192.0.0.255)
Public	192.0.3.0-192.167.255.255	Public	192.0.3.0-192.88.98.255 (ARIN)
			192.88.100.0-192.167.255.255 (ARIN)
			RFC3068: 6to4 Relay Anycast (192.88.99.0-192.88.99.255)
Public	192.169.0.0-196.255.255.255	Public	192.169.0.0-192.255.255.255 (ARIN)
			193.0.0.0-195.255.255.255 (RIPE NCC)
			196.0.0.0-197.255.255.255 (AfriNIC)
Dark Address	197.0.0.0-197.255.255.255 (IANA)	Public	196.0.0.0-197.255.255.255 (AfriNIC)

4.x Zones		5.0 Zones	
Public	198.20.0.0-213.255.255.255	Public	198.20.0.0-198.51.99.255 (ARIN)
			198.51.101.0-199.255.255.255 (ARIN)
			200.0.0.0-201.255.255.255 (LACNIC)
			202.0.0.0-203.0.112.255 (APNIC)
			203.0.114.0-203.255.255.255 (APNIC)
			204.0.0.0-209.255.255.255 (ARIN)
			210.0.0.0-211.255.255.255 (APNIC)
			212.0.0.0-213.255.255.255 (RIPE NCC)
			RFC5737: TEST-NET-3 (203.0.113.0-203.0.113.255)
Public	216.0.0.0-222.255.255.255	Public	216.0.0.0-216.255.255.255 (ARIN)
			217.0.0.0-217.255.255.255 (RIPE NCC)
			218.0.0.0-223.255.255.255 (APNIC)
Dark Address	223.0.0.0-223.255.255.255 (IANA)	Public	218.0.0.0-223.255.255.255 (APNIC)
Dark Address	27.0.0.0-27.255.255.255 (IANA)	Public	27.0.0.0-27.255.255.255 (APNIC)
Dark Address	49.0.0.0-50.255.255.255 (IANA)	Public	49.0.0.0-49.255.255.255 (IANA)
			50.0.0.0-50.255.255.255 (ARIN)

Index

D

downloading

- Console files 3

- Database files 2

- Manager files 2

- SmartConnector files 2

- Web files 3

downloading files 2

H

hierarchical manager

- upgrade 2

R

Related documentation 3

U

upgrade

- hierarchical manager 2

- preparing for 1

- steps 1

