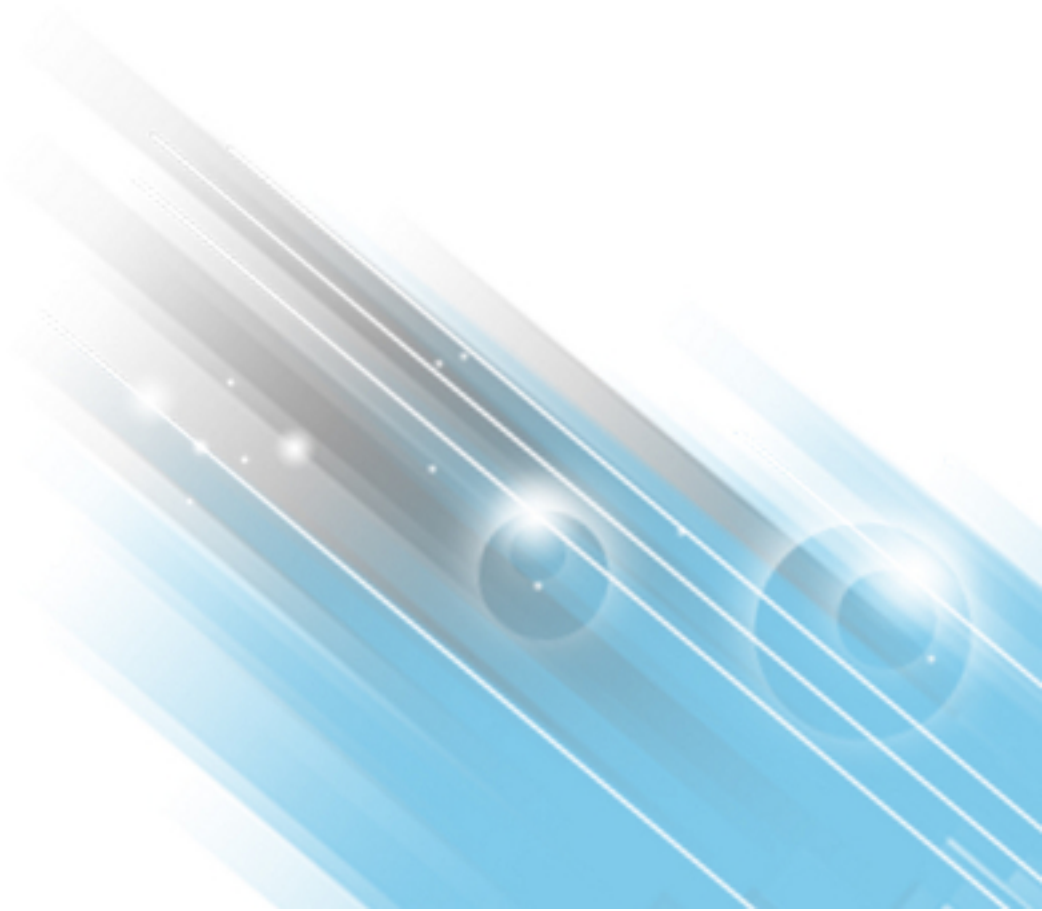
HP ArcSight ESM

Software Version: 6.8c

Upgrade Guide



April 24, 2015

Legal Notices

Warranty

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.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

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

Contents

Chapter 1: Preparing for the ESM 6.8c Upgrade

This document describes the steps required to upgrade the ESM software components from ESM 6.0c or 6.5c SP1 to ESM 6.8c. This section includes a summary and some essential prerequisites.

The following topics are covered here:

Summary

The following upgrade paths are supported for this release:

- ESM 6.0c Patch 3to ESM 6.8c
- ESM 6.5c SP 1 to ESM 6.8c

> **Caution: To upgrade your operating system...**
>
> To upgrade your operating system from Red Hat Linux 6.2 to 6.4 or 6.5, do so only before you upgrade your ESM installation to 6.8c. RHEL 6.2 is no longer supported. You can upgrade from RHEL 6.4 to 6.5 after upgrading to ESM 6.8c.

If you already have ESM and are licensed for the existing High Availability solution, there is a new High Availability module. It requires a new ESM license that supports it. The new High Availability module uses software to manage failovers and a different hardware configuration. Read the *High Availability User's Guide* and follow the instructions for upgrading ESM and installing the HA module as if you are a new HA user.

If you run into issues during upgrade, please contact HP ArcSight Customer Support for help.

Be sure to have the following handy while calling Support for help:

- the log files listed under the "Upgrade Log Files" on the next page section
- the system tables

```
/opt/arcsight/manager/tmp/
arcsight_dump_system_tables.sql.<timestamp>
```

Upgrade Log Files

The following log files get generated during the upgrade:

Suite Upgrade Logs:

- `/opt/arcsight/upgradelogs/suite_upgrade.log` - This log provides you with an overview of the upgrade progress. This is the first log that you should consult in the event your upgrade fails.
- `/opt/arcsight/suite/logs/install/ArcSight_ESM_6.8c_Suite_Install_<timestamp>.log`

Logger Upgrade Logs:

The log files are located in two directories:

- `/opt/arcsight/logger/current/arcsight/logger/logs` directory:
  - `logger_init_driver.log` - contains the Logger upgrade overview
  - `initmysqluser.log` - contains the Logger MySQL tables upgrade status
- `/opt/arcsight/logger/current/arcsight/logger/logs/postgressql_upgrade.out` - contains the Logger postgres tables upgrade output

Manager Upgrade Logs:

The log files are located in the `/opt/arcsight/manager/upgrade/out/ <timestamp>/logs/upgrade/` directory:

- `server.upgrade.log` - Manager upgrade log
- `server.upgrade.std.log` - Manager upgrade standard output

  The timestamp should be when you ran the upgrade. Each upgrade execution (described below) creates a log folder timestamp at the moment you ran it. Make sure to use the right one.

ArcSight Services Upgrade Logs:

The log files are located in the `/opt/arcsight/services/logs` directory:

- `arcsight_services.log` - contains information about starting/stopping services during upgrade
- `arcsight_services_async.log`

Installation Logs

The log files for each ESM component are located in the `/home/arcsight/` directory. The log file names are

- ArcSight_ESM_6.8c_Suite_Install_<timestamp>.log
- ArcSight_Logger_6.0_Install_<timestamp>.log
- ArcSight_ESM_Manager_6.8c_Install_<timestamp>.log

Planning Your Upgrade

Caution: Please be aware that once you begin the upgrade, you cannot roll back to the previous version of ESM. Do not attempt to use the uninstall link , it does not work for an upgrade. If you encounter errors when upgrading, contact HP ArcSight Customer Support for help to move forward with the upgrade process.

- If you have the space or perhaps space in a separate storage device, you can back up the entire `/opt/arcsight` directory.
- **Important!** Verify that your existing ESM is fully functional and its archives are intact. If there is any issue with your existing ESM system, contact HP ArcSight Customer Support before upgrading.
- To run the upgrade in GUI mode, Install the X Window system package if it is not already installed. This is optional.
  - Use xorg-x11-server-utils-7.5-13.el6.x86_64 or a later version for RHEL.
  - Use xorg-x11-server-7.4-27.81.7 or a later version for SUSE Linux.

  If the X Window package is not installed, the upgrade runs in console mode.
  If the upgrade does not run in the expected mode, see "Upgrading in Console or GUI Mode" on page 9.
- Both XFS and EXT4 file system formats are supported in ESM 6.8c. After upgrading, you remain on the same file system format you were on before. ESM does not support switching file system formats.
- Before you begin upgrading ESM, we recommend that you open a ticket with HP ArcSight Customer Support to test the upgrade with your system tables, to determine if any special steps are necessary for your configuration. Run the resource validator (`resvalidate`) **before** you provide Customer Support with your system tables. See the Caution below for details on running `resvalidate`. Fix **all** the invalid resources found by the resource validator before sending the system tables to Support. Allow two weeks for results when planning your deployment. Having HP ArcSight Customer Support test your upgrade will help make your upgrade run more smoothly.

  Caution: Run the resource validator (`resvalidate`) located on the ArcSight Manager in `/opt/arcsight/manager/bin/` directory to check that the resources are working correctly before the upgrade. This prevents you from attributing broken resources with the upgrade. Run the resource validation script as follows:

First run:

```
arcsight resvalidate
```

Then run:

```
arcsight resvalidate -persist false
```

- Standard, system-supplied resources are refreshed with new versions during upgrade. If you customized any of these resources, back them up in .arb files before you upgrade. See " Preparing Existing Content for Upgrade" on page 33 for details.
- The upgrade now requires an SSL certificate in the Manager's truststore for the ArcSight services client. It does this automatically, but if you changed the Manager's truststore password, the certificate import does not occur. The upgrade completes, but the Manager service status shows up as "initialized" indefinitely. If you changed your Manager truststore password, change it back to *changeit* before running the upgrade and restore your secure password after the upgrade.
- Download the upgrade file, `ArcSightESMSuite-xxxx.tar` from the HP SSO download web site. The xxxx in the file name stands for the build number. When you click on the .tar file to download it, its checksum appears at the bottom of the page. After downloading the .tar file, calculate the checksum on your downloaded .tar file and make sure it matches with the checksum provided on the download page.
- Make sure that you have at least 50 GB free disk space in your `/opt` directory.
- Make sure that you have at least 3 GB free disk space in your `/tmp` directory.
- If you have any connectors that are older than version 4.8.1, ArcSight recommends that you upgrade them to the latest version.
- The file `/opt/arcsight/logger/data/mysql/my.cnf` is retained by the upgrade, so any customizations you made remain. The upgrade creates a new, suggested version called `my.cnf.sug`. After the upgrade, compare the two to see if you want to adopt any of the suggested changes.

Install Time Zone Package

ESM uses the time zone update package in order to automatically handle changes in time zone or changes between standard and daylight savings time. During installation, ESM checks to see if the appropriate operating system time zone package is installed. If it is not, you have the option of exiting the installer to install the latest operating system timezone update or continuing the ESM installation and skipping the timezone update for ESM components. We recommend installing the time zone update package.

- For RHEL 6.4/6.5 and CentOS 6.5 use `tzdata-2014f-1.el6.noarch.rpm`.
- For SuSE 11.x use `timezone-2014f-8.1`.
  When installing the timezone package on SuSE, some dependencies need to be resolved. Please check with your system administrator if you have a problem resolving these dependencies.

In both cases, the "f" can be f or any later version. To install them use the command:
`rpm -Uvh <package>`

You should also check to make sure that the `/etc/localtime` link is pointing to a valid time zone. To do that, run the following command:

```
ls -altrh /etc/localtime
```

You should get a response similar to this (below), where <ZONE> is your time zone such as America/Los_Angeles.

```
lrwxrwxrwx. 1 root root 39 Nov 27 08:28 /etc/localtime ->
/usr/share/zoneinfo/<ZONE>
```

If this is not correct, run the following commands as user *root*:

```
source /etc/sysconfig/clock
mv /etc/localtime /etc/localtime.old
ln -s /usr/share/zoneinfo/<ZONE> /etc/localtime
```

Verify that `/etc/localtime` is pointing to the correct time zone or use the `date` command.

If you quit the installation to fix these, you can simply run the installation again.

If you complete the installation without fixing these, you can still set up the time zone package after completing the installation. Use the following procedure after ensuring that you have downloaded and installed the correct package and the link is set correctly. (Remember, this is for after the installation is complete.):

1. As user *arcsight*, shut down all arcsight services. (This is important.) Run
   `/opt/arcsight/services/init.d/arcsight_services killAllFast`
2. As user *root*, run the following command (this is one line):

   ```
   /opt/arcsight/manager/bin/arcsight tzupdater /opt/arcsight /opt/arcs
   ight/manager/lib/jre-tools/tzupdater
   ```
3. Monitor for any failure.
4. Restart all arcsight services.

Upgrading in Console or GUI Mode

The upgrade automatically detects whether you have a GUI environment installed. It runs in GUI mode if the GUI environment is installed and in console mode if it is not. Under some circumstances, the configuration of your UI environment can be ambiguous to the extent that it is not sufficiently installed

to enable the upgrade to run in GUI mode, but there are components present that prevent it from running in console mode. These topics address that situation:

Upgrading in Console Mode

To ensure that the upgrade starts in console mode, execute the following command in a command window:

```
export ARCSIGHT_JVM_OPTIONS="$ARCSIGHT_JVM_OPTIONS -Djava.awt.headless=true"
```

The heap memory for the upgrade process is now set to 6 GB. It is advisable to change this value to be the same as your Manager heap size. To change it, use this command:

```
export ARCSIGHT_JVM_OPTIONS="$ARCSIGHT_JVM_OPTIONS -Xmx<heap_size>m -
XX:+HeapDumpOnOutOfMemoryError"
```

`-Xmx<heap_size>m` is the heap size in megabytes. This heap size setting is only used during the upgrade.

To set heap memory to 8 GB, for example, you would set `-Xmx<heap_size>m` to `-Xmx8192m`.

Run the upgrade.

Upgrading in GUI Mode

If your X Window configuration is incorrect, the upgrade process cannot run in GUI mode. If that is the case, the upgrade script provides a message to that effect, and gives you an opportunity to cancel it. If the UI environment is configured such that the upgrade does not automatically start in GUI mode, and you want it to, fix your UI installation and try again.

Chapter 2: Upgrading the ESM Manager

Caution: Be aware of these three cautions:

- If you would like to upgrade your operating system from Red Hat Linux 6.4 to 6.5, do so only **after** upgrading to 6.8c.
- If you run the upgrade from a remote system connected to the ESM system, have X-Windows running on your remote system. Use ssh -X to run the upgrade.
- Do not modify any environment variables. Particularly, if Logger environment variables such as ARCSIGHT_LOGGER_BASE, UPGRADE and ARCSIGHT_BASE are altered, the upgrade may fail.

Untar the Installation .tar File

1. Log in as user *arcsight*.
2. Make sure the downloaded the .tar file is on the system you intend to upgrade to ESM 6.8c .
3. Verify the integrity of the .tar file just to make sure that it was not truncated or corrupted during the download. Run:

   ```
   md5sum -c ArcSightESMSuite-xxxx.tar.md5
   ```

4. Untar the `ArcSightESMSuite-xxxx.tar` file:

   ```
   tar xvf ArcSightESMSuite-xxxx.tar
   ```

Remove ArcSight Services

Before you run the upgrade, remove the ArcSight services. To do so:

1. Switch user to *root*:

   ```
   su - root
   ```

   Enter the password for the user *root* when prompted.

2. Run the following command to remove the ArcSight services:

   ```
   /opt/arcsight/manager/bin/remove_services.sh
   ```

Removed services are added back later when you run the `setup_services.sh` command at the end of the upgrade process.

Keep these TCP Ports Open

Before upgrading ESM, open the following TCP ports on your system if not already open and ensure that no other process is using these TCP ports.

Open the following TCP ports for external incoming connections:

8443
9443
9000

The following TCP ports are used internally for inter-component communication by ESM. Make sure that they are open and NOT in use:

1976, 28001, 2812, 3306, 5555, 6005, 6009, 6443, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8766, 8808, 8880, 8888, 8889, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9095, 9090, 9123, 9124, 9999, 45450

Running the Upgrade Process

To upgrade the components in your existing ESM installation:

1. Log in as user *arcsight*.
2. Provide execute permission to `ArcSightESMSuite.bin` file:

   ```
   chmod +x ArcSightESMSuite.bin
   ```

3. Run the upgrade:

   ```
   ./ArcSightESMSuite.bin
   ```

   Before the upgrade process begins, it checks to make sure that all requirements for the upgrade are met. Should you encounter an error at this point, fix the error and run the upgrade file again.

   Under some circumstances, users on SuSE Linux might get an error at this point that says, “The required port 2812 is still in use.” If you get this error, simply reboot your system and rerun the upgrade.

4. It asks you to confirm that you want to upgrade your existing ESM installation. Click **Yes**:

   Note: Should you run into errors after the upgrade begins...

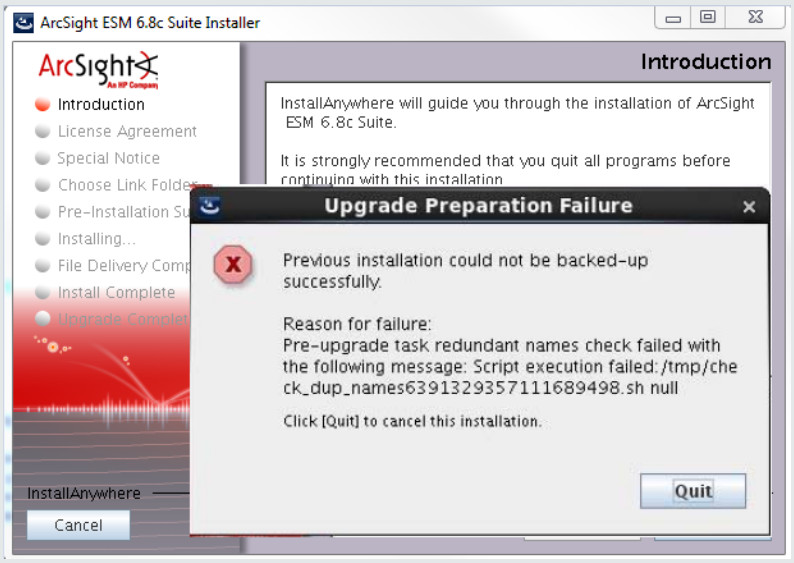
Check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file to see where the upgrade failed. If your log file does not have the following line in it, you can fix the error that you see in the log file and rerun the upgrade:

```
Preupgrade tasks completed successfully.
```

If the upgrade failed at any point after the preupgrade tasks, contact HP ArcSight Customer Support for help with recovering from the failure and send all the `/opt/arcsight/upgradelogs/*` to them.

Do not use the uninstall link, it does not work for upgrades.

Note: The upgrade does a Pre-upgrade redundant-name check to ensure there are no duplicate resource names in the same group in your database. If it finds duplicate names, it generates an error that causes the upgrade to halt.



To resolve this:

a. Check the `/opt/arcsight/upgradelogs/runcheckdupnames.txt` file to see which duplicate names are causing the conflict.

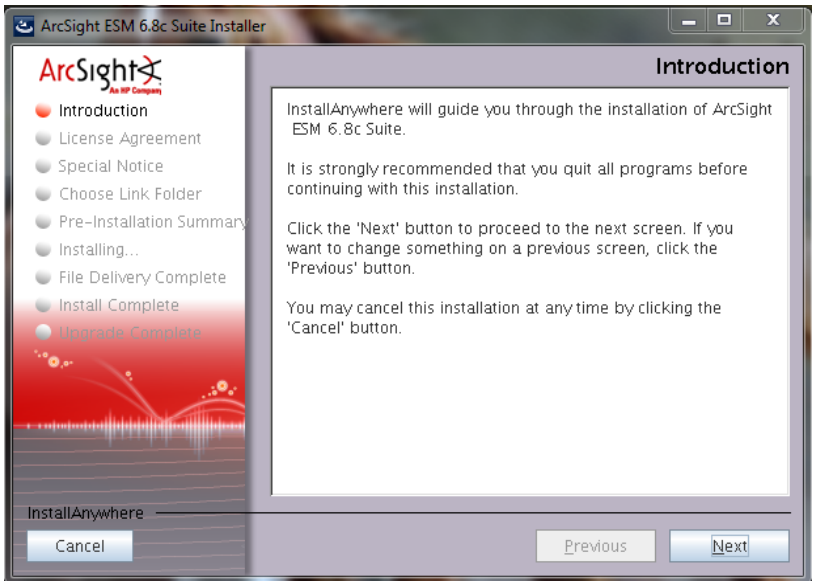
b. Resolve duplicate names manually.

c. Re-run the upgrade from "Run the upgrade:" on the previous page.

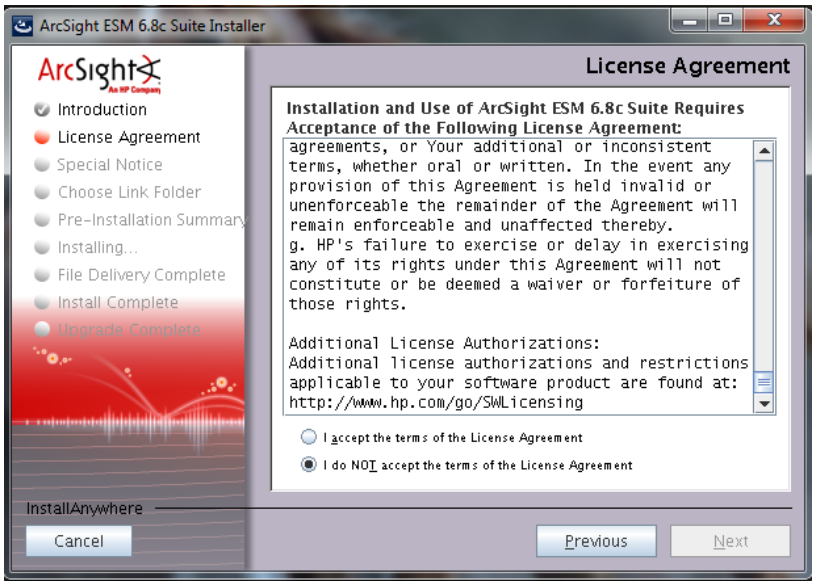
Please contact Customer Support using the HP SSO website if you need assistance doing this.

Note: If you are using SUSE linux, and you get a message saying, “The required port 2812 is still in use,” reboot the server to clear this condition and re-run the upgrade.

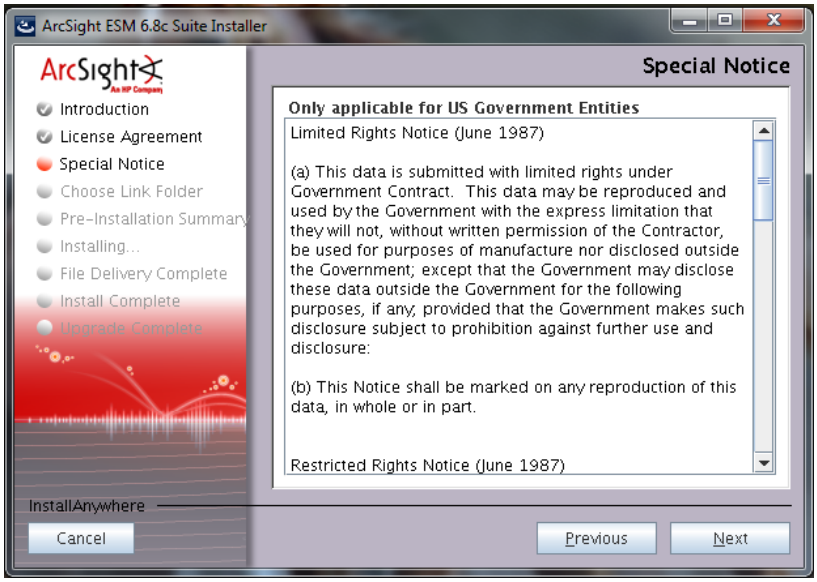
5. Read through the Introduction screen and click **Next**:



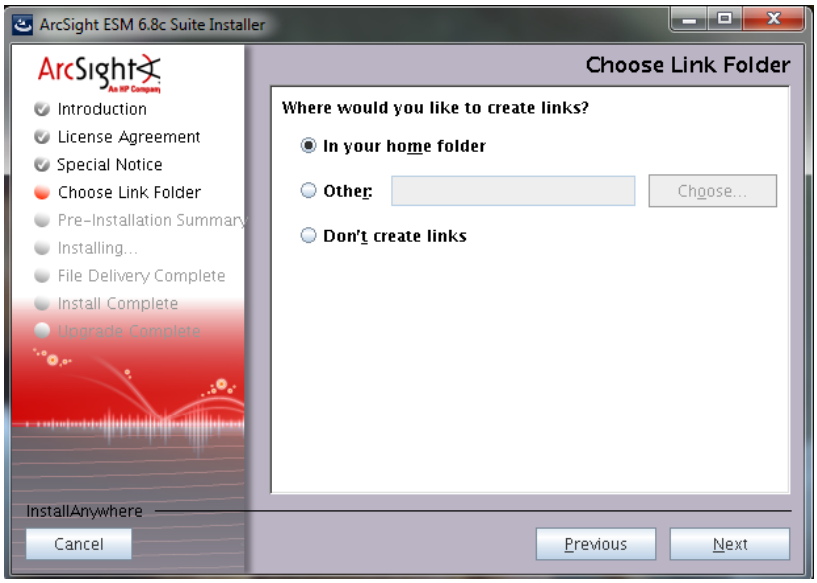
6. Click the “I accept the terms of the License Agreement” radio button then click **Next**. The button is not active until you hace scrolled to the bottom of the license agreement.



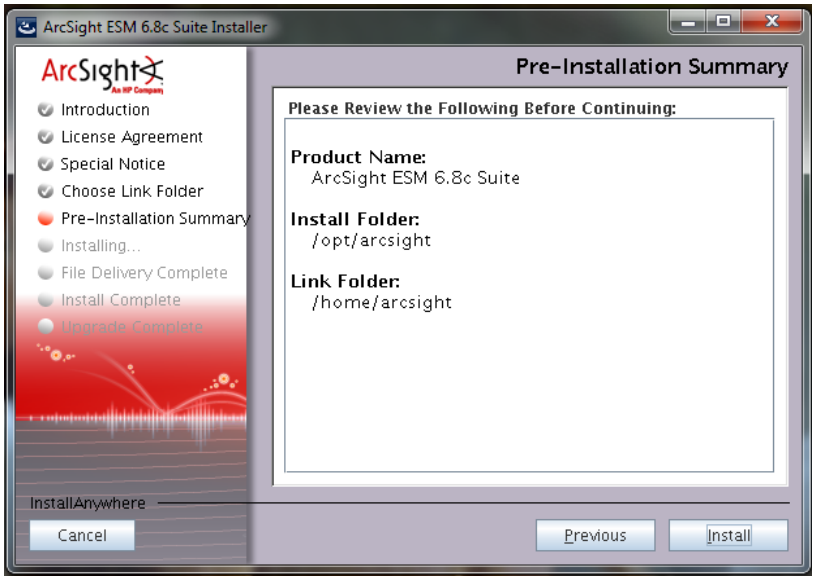
7. Read the notice and click **Next**:



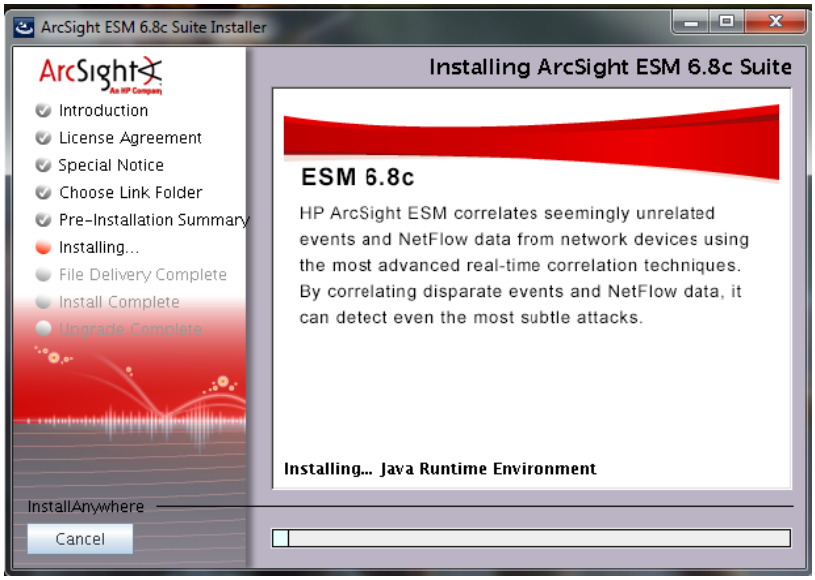
8. Specify or select where you would like the link for the installation to be created and click **Next.**



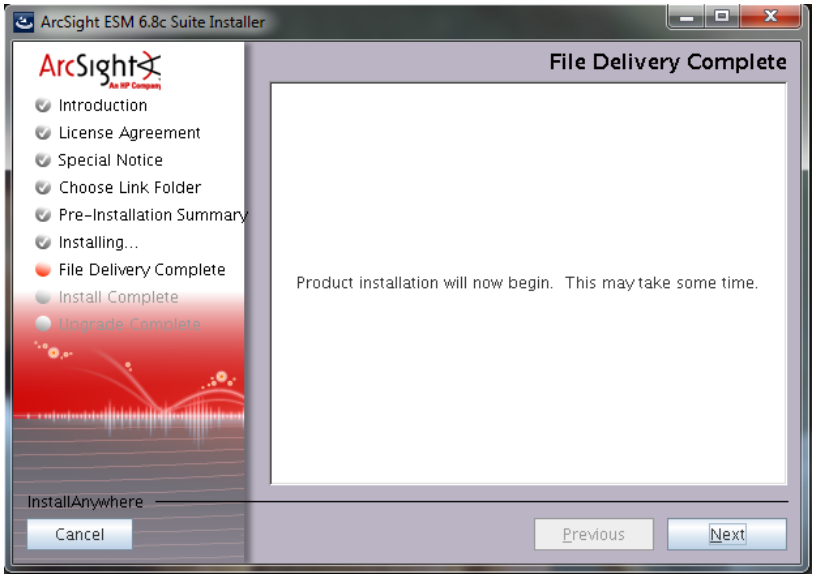
9. Review the settings and click **Install**.



10. You will see the following progress bar:



11. Once the bits for all components have been copied over, you get the following screen. Click **Next**:



The upgrade is done in silent mode and transfers configurations, upgrades the schema, and upgrades the content.

- Before the upgrade process begins, the existing software components will be backed up into the `/opt/arcsight` directory:
  - `manager.preUpgradeBackup`
  - `services.preUpgradeBackup`

- `suite.preUpgradeBackup`
- `/opt/arcsight/logger/BLxxxx`

  where xxxx is the Logger version number.

- See the section, "Upgrade Log Files" on page 6 for log files that get generated during the upgrade.
- The system tables are exported into `/opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql.<timestamp>`

  Caution: Do not delete the dump file before the upgrade is completely done and confirmed to be good. You will need it to recover in case of a failed upgrade.

- For upgrade from ESM 6.5c SP1, the postgres dump can be found in `/opt/arcsight/logger/current/arcsight/logger/user/logger/esm65c.postgres.<timestamp>.dump`

  For upgrade from ESM 6.0c P3, the postgres dump can be found in `/opt/arcsight/logger/current/arcsight/logger/user/logger/esm60c.postgres.<timestamp>.dump`

12. The installation program shows you the progress as the components get installed and the upgrade begins.
13. You will see the **Upgrade Complete** screen once the upgrade is finished. Click **Done**.
14. **Important!**
    Make sure to run the following as user *root*:

    ```
    su - root
    ```

    Enter the root password when prompted.

    ```
    /opt/arcsight/manager/bin/setup_services.sh
    ```

15. Follow applicable post-upgrade steps listed in the section, "Post-Upgrade Tasks" on page 20.

Handling a Time Zone Update Error

There are two possible errors that can happen when the installer tries to update the time zone information for the ESM components.

1. A timezone version 2014f or later rpm for your operating system is not installed.
2. The /etc/localtime link is pointing to invalid or non-existent timezone.

You can choose to continue with the installation even if the right timezone package is unavailable or incorrectly setup. If you choose to do so, you can update timezone info for the ESM components post-installation. Refer to "Install Time Zone Package" on page 8, to correct one of these time zone issues.

To Confirm that the Upgrade Succeeded

You can check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file, which will show the error in case of a failed upgrade.

You can check the upgrade summary report and logs to find out if the Manager upgraded successfully. The upgrade summary report is applicable to the Manager only and can be found in the Manager's `<ARCSIGHT_HOME>/upgrade/out/<time_stamp>/summary.html`.

When upgrade succeeds, you should see the following in the `/opt/arcsight/upgradelogs/suite_upgrade.log` file:

```
Upgrade completed successfully.
```

Be sure to check if all the components are up by running the following command:

```
/etc/init.d/arcsight_services status all
```

You should see a response similar to the following:

```
aps service is available
execprocsvc service is available
logger_httpd service is available
logger_servers service is available
logger_web service is available
manager service is available
mysqld service is available
postgresql service is available
```

This command also shows the versions of the components installed which is another good way to verify a successful upgrade:

Build versions:

```
esm:6.8.0.xxxx.0(BExxxx)
storage:BLxxxxx
```

Run the following command to check the RPM versions:

```
rpm -qa|grep arcsight
```

You have upgraded to ESM 6.8c.

Make sure to upgrade your existing Console. See "Upgrading ArcSight Console" on page 22.

If the Manager service shows up as "initialized" indefinitely, it probably means you did not change the Manager's truststore password back to *changeit*, before running the upgrade. If that's the case, run the following two commands as user *arcsight* to import the `arcsight_services`' certificate to the Manager's truststore:

1. Stop the Manager. (Skip the timeout message when stopping the Manager).
2. `cd /opt/arcsight/manager/bin`
3. `./arcsight keytool -store managercerts -importcert -alias services_admin -file /opt/arcsight/manager/config/service-certificate.cer -noprompt`
4. Restart the Manager.

Post-Upgrade Tasks

After you have confirmed that the upgrade was successful, you can perform the tasks in this section.

- After the upgrade is complete, clear the following folders:
  `/opt/arcsight/manager/user/manager/datamonitors/checkpoints`
  `/opt/arcsight/manager/user/manager/rules/checkpoints`
- The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors, which are not currently installed with ESM6.8c.
- Decide whether to merge the suggested my.cnf file that comes with the upgrade with your existing `my.cnf` file, which is still in use. The upgrade does not overwrite your `my.cnf` file, so that if you have any customizations they are preserved. The my.cnf file that the upgrade adds is called `my.bak.sug`. If you have not made any customizations to your `my.cnf` file, you probably do not need to make any changes. If you have made customizations, compare your `my.cnf` file to the `my.bak.sug` that comes with the upgrade and decide which properties to change, if any.

  To use the Forwarding Connector, download the installation files for it and install it manually. Refer to the Forwarding Connector documents to do so.
- The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors, which are not currently installed with ESM 6.8c.
  - ArcSight IP Flow SmartConnector
  - ArcSight QoSient ARGUS SmartConnector

    When upgrading to ESM 6.8c if you want to use the NetFlow Monitoring content, you need to install and configure these SmartConnectors. For information about how to obtain the SmartConnectors, contact your HP ArcSight sales representative.
- File resources are not handled properly during the ESM upgrade. This results in unassigned file

resources after the upgrade. For example, the .art files are created as new file resources in ESM 6.8c, and the resources get new version IDs during the upgrade. The original files are stored in the Files resource under the Unassigned folder. To work around this issue, you can safely delete the unassigned `.art` files after an upgrade because they are duplicates.

- The upgrade preserves customized velocity templates by adding the `.previous` file extension and replaces the original file with an un-customized version. To restore your customized version, simply delete the new file and change the name of your customized version by removing the `.previous` file extension.

  For example, if you customized the file `email.vm`, there are two files after the upgrade completes: `email.vm` and `email.vm.previous`. Your customizations are in the second one, which is not being used. To restore your customized version, delete `email.vm` and rename `email.vm.previous` to `email.vm`.

- If you changed the Manager's truststore password from your secure password back to “changeit” before running the upgrade, restore the Manager's truststore password to your secure password, and restart the Manager.

- If you customized the Cases UI on the existing 6.x environment, the customizations are not copied over automatically during the upgrade. The upgrade creates backups of several files and places them in preUpgradeBackup folders. Most of these are restored correctly after the upgrade; in this release a few are not. The workaround is to restore them manually after the upgrade as follows:

  a. Copy `label_strings_en.properties` and `resource_strings_en.properties` under `/opt/arcsight/manager.preUpgradeBackup/i18n/common` to `/opt/arcsight/manager/i18n/common`.

  Note: For English, if the `*_en.properties` file does not exist under `/opt/arcsight/manager.preUpgradeBackup/i18n/common`, copy the `*.properties` file. If it exists, copy `*_en.properties`. For other locales, copy the `*_<locale>.properties` file.

  b. Copy `caseui.xml` under `/opt/arcsight/manager.preUpgradeBackup/config` to `/opt/arcsight/manager/config`.

  c. If a customized case details mapping to audit events exists, copy `case.properties` under `/opt/arcsight/manager.preUpgradeBackup/config/audit` to `/opt/arcsight/manager/config/audit`.

  d. Restart the Manager for these changes to take effect.

Chapter 3: Upgrading ArcSight Console

The ArcSight Console upgrade process should be performed on all ArcSight Console instances that connect to the Manager running on the upgraded system.

1. Stop ArcSight Console if it is running.
2. Download the appropriate installation file for your platform from the HP SSO download web site. The xxxx in the filename represents the Console build number:
   - `ArcSight-6.8.0.xxxx.0-Console-Win.exe`
   - `ArcSight-6.8.0.xxxx.0-Console-Linux.bin`
   - `ArcSight-6.8.0.xxxx.0-Console-MacOSX.zip`
3. If you downloaded the 6.8c Console installation file to a different machine, transfer it to the machine on which you plan to install the Console.
4. Run the installation file appropriate for your platform:
   - **On Windows**:
     Double-click `ArcSight-6.8.0.xxxx.0-Console-Win.exe`
   - **On Macintosh:**

     Unzip the following file:

     `ArcSight-6.8.0.xxxx.0-Console-MacOSX.zip`

     and run the installer by double-clicking on it.

     On the Macintosh, it does not import the certificate, even if you selected to transfer settings. After the upgrade, when you connect to the Manager, it prompts you to import the certificate again. Just click **OK**, and the Console completes the import operation.
   - **On Linux**:

     Run the following command, which you must do as a non-root user.

     `./ArcSight-6.8.0.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-6.8.0.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 6.8c that is different from where the existing Console is installed.

  Note: Do NOT install the new Arcsight Console in the same location as the existing ArcSight 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.

5. The Console installation program prompts you for 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 or IP address and port number, and authentication information including authentication type. Select **Yes, I want to transfer the settings** and click **Next.**
6. 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.

   Click **Next**.
7. See the ESM Installation and Configuration Guide for details on the remaining screens for installing a Console using the installation wizard.
8. Start the ArcSight Console.

9. After you have upgraded a Console to 6.8c:

   a. You can view the upgraded standard content

   b. All your SmartConnectors are connecting to the Manager on the ESM system.

   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.

Chapter 4: Checking Existing Content After Upgrade

After the upgrade is completed, verify that all your content has been successfully transferred to the 6.8c structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

- **Check for resources under Unassigned**. Check the Unassigned group in the resource tree for all resource types. The Unassigned groups in each resource type contain any customer-created resources that were located in the previous ESM's “System” group.

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

- **Restore customizations to Standard-Content resources**. Standard Content is a set of system-supplied resources that are refreshed with new versions during upgrade. If you customized any of these system-supplied resources, your customizations were overwritten during the upgrade. Restore your configurations manually by importing the backed up .arb files you saved before you upgraded.

- **Reinstall mandatory packages.** If you upgraded from ESM 6.0c, there are two mandatory packages that are not installed by default:

  - /All Packages/ArcSight Administration/ArcSight Admin DB CORR
  - /All Packages/ArcSight Administration/ArcSight Search Filters

  Install them manually.

- **Check for assets under Disabled**. The Disabled group in the assets resource tree is dynamic, which means it queries the Manager every two minutes for assets that have been disabled. After the upgrade, check if any assets were disabled and moved to the Disabled group in the Assets resource tree.

  - If so, review the disabled asset to see the reason it was disabled and fix it as appropriate. For example, if an asset’s IP address is outside the range of the upgraded zone, either expand the range of the zone, or assign the asset to another zone.
  - You can also delete an asset that has become disabled if it is no longer needed (right-click the asset and select **Delete**).

  For existing assets, if two assets **in the same zone** have the same host name or IP address, one of them becomes invalid after the ESM upgrade to 6.8c. This may happen for assets whose host

names are Fully Qualified Domain Name (FQDN) of the asset. In 6.8c, only the host name is extracted from the FQDN and used when comparing the two assets.

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

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

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

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

  After the upgrade, verify that your user ACLs are correct and still valid based on how ArcSight standard content is organized for 6.8c. For example, Administrator access should only be granted to those with authority to work with system-level content, such as for `ArcSight System` and `ArcSight Administration`. Update user ACLs manually as appropriate.

- **Zones resource**. Check if any zones were invalidated during the upgrade process.

  - Fix zones that you want to keep but may have been rendered invalid during the upgrade.
  - Verify that the assets assigned to zones that have been moved or invalidated during the upgrade retain their connections to appropriate 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 6.8c 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 the Manager's <`ARCSIGHT_HOME>/upgrade/out/<time_stamp>/summary.html` to find invalid resources and fix their conditions as appropriate.

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

  An example would be of a rule that uses an ArcSight System filter whose conditions have been changed such that the rule matches more events than you expect, or doesn't match the events that you expect it to match. 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 6.8c, 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 the 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 previous ESM 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 6.8c 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 (the previous ESM) form. Resources moved to this folder are still active, so if you rely on any of these resources, they will still be present and operational.

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

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

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

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

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

HP also recommends that you verify whether the new 6.8c resources address the same goal more efficiently.

After upgrading to ESM 6.8c, you can generate a list of deprecated resources using the Find Resource function:

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

Chapter 5: Upgrading ArcSight SmartConnectors

The SmartConnectors must be running version 4.8.1 or later. However, HP strongly recommends that you upgrade all connectors to the latest available release.

Download installation files as appropriate for your SmartConnector platforms. 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 steps 3 and 4 for every SmartConnector you identified in step 1.

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

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

Upgrading the Forwarding Connector

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

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

Chapter 6: Upgrading Hierarchical or Other Multi-ESM Installation to 6.8c

This chapter describes the method for upgrading a multi-ESM deployment to 6.8c.

Summary

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

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

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

Upgrading a Hierarchical Deployment

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

1. Upgrade any SmartConnectors that are not running a recent version. For best results, use version 4.8.1 or later.
2. Remove the ArcSight services on the current ESM.
3. Follow instructions in the "Preparing for the ESM 6.8c Upgrade" on page 5 to upgrade your ESM to 6.8c.
4. Once ESM 6.8c is running, follow instructions in the "Upgrading ArcSight Console" on page 22 to upgrade any Consoles connected to it.
5. Upgrade the Forwarding Connector connected to this ESM to Forwarding Connector 7.0.7.7286.0.

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

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

Upgrading a Peer-to-Peer Configuration

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

Chapter 7: Upgrading Standard Content

This chapter discusses the following topics.

Preparing Existing Content for Upgrade

The majority of standard content does not need configuration and does not require special preparation for upgrade. Upgrade preparation is recommended only for content that has been configured and for which configuration is not preserved after the upgrade.

Note: If a resource has been deleted in the release to which you are upgrading, it is moved during upgrade to a folder in the resource tree called Deprecated. For example, All Rules/Arcsight System/Deprecated. If you use this deprecated resource, move it to your own group after the upgrade.

Configurations Preserved During Upgrade

The following resource configurations are preserved during the upgrade process. No restoration is required for these resources after the upgrade.

- Asset modeling for network assets, including:
  - Assets, and asset groups and their settings
  - Asset categories applied to assets and asset groups
  - Vulnerabilities applied to assets
  - Custom zones
- SmartConnectors
- Users and user groups
- Report schedules

- Notification destinations and priority settings
- Cases

Configurations that Require Restoration After Upgrade

The following resource configurations require restoration after upgrade.

- Any standard content resource that you have modified, including active lists

  Note: Only active list attributes, such as the TTL and description are not preserved during upgrade. Any entries removed from an original active list are restored during upgrade. Any entries added to an active list are preserved during upgrade.

- Any custom content or special modifications not already described in this document (including customizations performed by Professional Services)

Backing Up Existing Resources Before Upgrade

Before you back up existing resources, run the resource validator (`resvalidate.sh`) located on the ESM Manager in the Manager's `/opt/arcsight/manager/bin` to check that the resources are working correctly before the upgrade. This prevents you from attributing broken resources with the upgrade.

During the upgrade process, the content is run through a resource validator automatically (see " Fixing Invalid Resources" on page 36).To help the process of reconfiguring resources that require restoration after upgrade, back up the resources you identify in "Configurations that Require Restoration After Upgrade" above and export them in a package. After upgrade, you can re-import the package and use the existing resources as a reference for restoring the configurations to the upgraded environment.

To create a backup of the resources that require restoration after upgrade:

1. For each resource type (filter, rule, active list), create a new group under your personal group. Provide a name that identifies the contents.
   - Right-click your group name and select **New Group**.
2. Copy the resources into the new group. Repeat this process for every resource type you want to back up.
   - Select the resources you want to back up and drag them into the backup folder you created in step 1. In the Drag & Drop Options dialog box, select **Copy**.
3. Export the backup groups in a package.

- In the Navigator panel Packages tab, right-click your group name and select **New Package**. In the Packages editor in the Inspect/Edit panel, name the package to identify the contents.
- Select the group that you created in step 1, right click and select **Add to Package**. Select your new package and click **OK**.
- Right click your package name and select **Export Package to Bundle**.

> **Tip: Copy and paste configurations from the old resources to the new**
>
> Instead of overwriting the new resources with backup copies of the old ones, copy and paste configurations from the old resources one by one into the new ones. This procedure ensures that you preserve your configurations without overwriting any improvements provided in the upgrade.

Performing the Upgrade

After exporting a copy of the configured resources in a backup package, you are ready to perform the upgrade process. Refer to "Preparing for the ESM 6.8c Upgrade" on page 5 for upgrade procedures.

Checking and Restoring Content After Upgrade

After the upgrade is complete, perform the following checks to verify that all your content has been transferred to the new environment successfully.

Verifying and Reapplying Configurations

Verify and restore standard content after the upgrade.

1. Verify that your configured resources listed in the section "Configurations Preserved During Upgrade" on page 33 retained their configurations as expected.
2. Reconfigure the resources that require restoration.
   a. Re-import the package you created in "Backing Up Existing Resources Before Upgrade" on the previous page.
   b. One resource at a time, copy and paste the configurations preserved in the package of copied resources into the new resources installed with the upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old ensures that you retain your configurations without overwriting any improvements provided with the upgraded content.

Verifying Customized Content

It is possible during upgrade that updates to the standard content cause resources you created to work in a way that is not intended. For example, a rule might trigger too often or not at all if it uses a filter in which conditions have been changed.

To verify that the resources you rely upon work as expected, check the following:

- **Trigger events**. Send events that you know trigger the content through the system using the Replay with Rules feature. For more about this feature, refer to the *ArcSight Console User's Guide*.
- **Check Live Events**. Check the Live or All Events active channel to verify that the correlation event triggered. Check that the data monitors you created are returning the expected output based on the test events you send through.
- **Verify notification destinations**. Verify that notifications are sent to the recipients in your notification destinations as expected.
- **Verify active lists**. Check that any active lists you have created to support your content are gathering the replay with rules data as expected.
- **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. Find invalid resources and fix their conditions as appropriate. For more about invalid resources, see " Fixing Invalid Resources" below.

Fixing Invalid Resources

 During the upgrade process, the content is run through a resource validator, which verifies that the values expressed in the resource condition statement still apply to the resource in its new format, and that any resources upon which it depends are still present and also valid. The resource validator runs on any resource that contains a condition statement or populates the asset model, such as:

- Active channels
- Filters
- Data Monitors
- Rules
- Report queries and schedules
- Assets and Asset ranges
- Zones

It is possible that during upgrade, the condition statement for a resource you created or modified becomes invalid. For example, if the schema of an ArcSight-supplied active list changes from one release to another and a resource you created reads entries from this list, the condition statement in the created resource no longer matches the schema of the active list, and the logic is invalid.

When the installer performs the resource validation check and finds an invalid resource, it identifies why the resource is invalid in the report it generates at the end of the upgrade. The upgrade installer:

- Saves the reason the resource is found to be invalid in the database so you can generate a list of invalid resources that you can use later to repair the problems manually.
- Disables the resource so it does not try to evaluate live events in its invalid state.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Upgrade Guide (ESM 6.8c)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!