

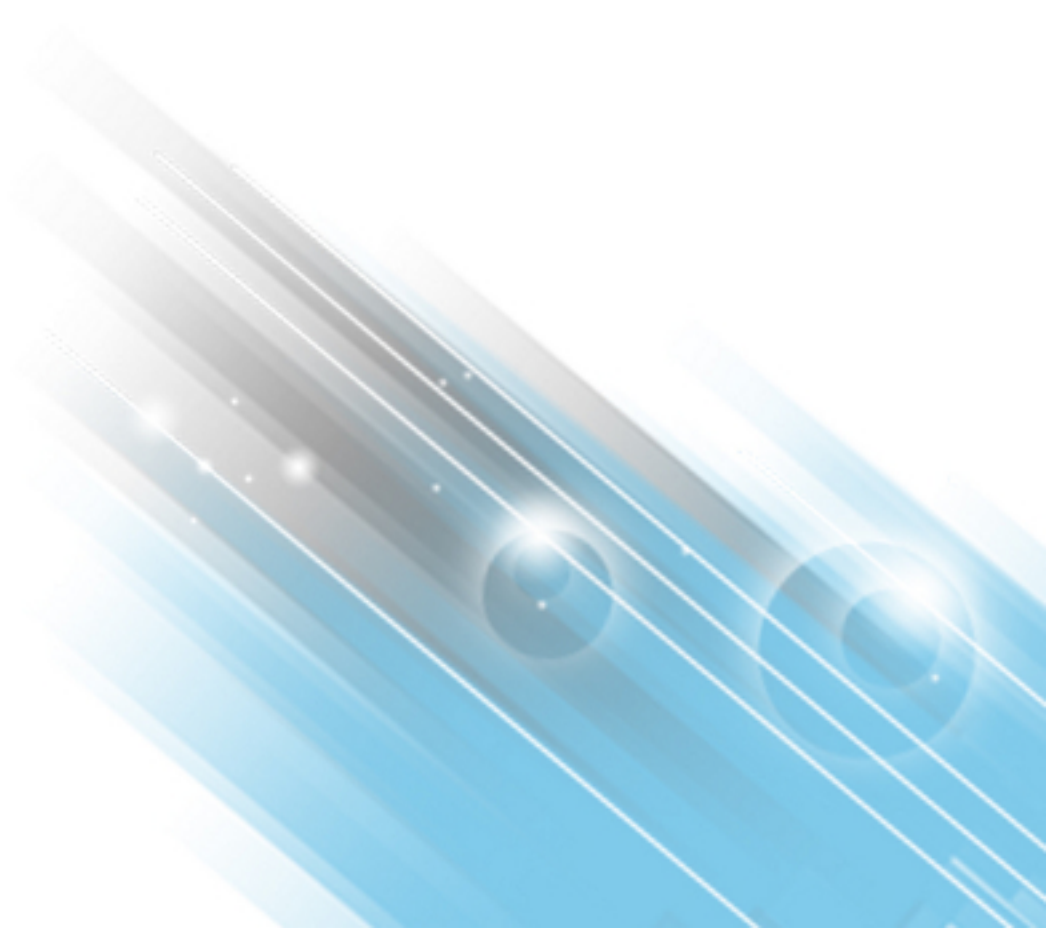


HP ArcSight ESM

Software Version: 6.9.1c

Upgrade Guide

July 21, 2016



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

© Copyright 2016 Hewlett-Packard Development Company, L.P.

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

<https://www.protect724.hpe.com/docs/DOC-13026>

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://www.protect724.hpe.com

Contents

Chapter 1: Preparing for the Upgrade	5
Verify Proper Operation	5
In Case of Problems	5
Prepare Resources for Upgrade	6
Validate Resources	7
Back up Resources Before Upgrade	8
Open a Ticket with Support	9
Avoid X Windows	9
Convert Pager Numbers to Emails	10
Restore Default Manager Truststore Password	10
Use the Same File System - Software ESM	10
Set Disk Space - Software ESM	10
Set Java (Manager) Heap Size	10
Install the Time Zone Package - Software ESM	11
Review High Availability Module Upgrade - Software ESM	12
Download the Upgrade Utilities Package	12
Chapter 2: Running the Upgrade	13
Upgrade Software ESM to ESM 6.9.1c	13
Upgrade ArcSight Express to ESM Express 6.9.1c	15
Migrate Connector Appliance and Connector Data to ArcSight Management Center - ArcSight Express Only	16
Before Performing the Migration	16
The Data Migration Process	17
Backing Up Your Connector Appliance and Connector Data on ArcSight Express. .	17
Restoring Your Connector Appliance and Connector Data to ArcMC	17
Delete Unneeded ArcSight Express Directories	18
Upgrade the AE Operating System	19
Upgrade ArcSight Express to ESM Express	20
Upgrade ESM Express to ESM Express 6.9.1c	22
Confirm that the Upgrade Succeeded	23
Post Upgrade Tasks	24
Install Time Zone Package - Software ESM	25
Fix Invalid Resources	25
Install Netflow SmartConnectors	26
Supply Email Addresses for Converted Pager Destinations	26
Delete Unassigned File Resources	26

Restore Deprecated Resources	26
Restore Custom Velocity Templates	26
Restore Custom Case UI	27
Checking and Restoring Content After Upgrade	27
Verify and Reapply Configurations	27
Verify Customized Content	28
Chapter 3: Upgrading ArcSight Console	29
Run the ESM 6.9.1c Console Installation	29
Run the ESM 6.9.1c Console Configuration	31
Post-Console-Upgrade Tasks	31
Chapter 4: Checking Existing Content After Upgrade	32
Chapter 5: Upgrading ArcSight SmartConnectors	36
Upgrade the Forwarding Connector	36
Chapter 6: Upgrading Hierarchical or Other Multi-ESM Installation to 6.9.1c	37
Summary	37
Upgrading a Hierarchical Deployment	37
Upgrading a Peer-to-Peer Configuration	38
Send Documentation Feedback	39

Chapter 1: Preparing for the Upgrade

This document describes the steps required to upgrade software ESM, ArcSight Express, or ESM Express to version 6.9.1c. This section includes a summary and some essential prerequisites. The supported upgrade paths are:

- From ESM 6.5c SP1 or 6.8c (with the latest patch is recommended). You must first upgrade the operating system to RHEL 6.7.
- From ArcSight Express 4.0 P1 or later on a B7500 appliance. You must first upgrade the operating system to RHEL 6.7. If you installed the security update of January 7, 2016, that fixes bug NGS-15050, you *must* uninstall it before you upgrade. Instructions are in the documentation that came with the security update. Uninstall *only* the security update. Do not uninstall Patch 1.
- From ESM Express 6.9.0 on RHEL 7.1 on a B7600 appliance.

SuSE Linux is no longer a supported operating system platform for ESM. Therefore, upgrades from ESM 6.5c SP1 or 6.8c on SuSE to ESM 6.9.1 are not supported.

For details on supported platforms, refer to the [HPE ArcSight ESM Support Matrix](#) available on Protect 724.

Verify Proper Operation

Verify that your existing ArcSight Express, ESM Express, or ESM is fully functional and its archives are intact. If there is any issue with your existing system, contact HPE ArcSight Customer Support before upgrading.

In Case of Problems

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

Have the system tables available when calling Support. Refer to the `arcsight` command `export_system_tables`, which is described in the "Administrative Commands" section of the *ESM Administrator's Guide*. The output looks like this:

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

Have the log files available when calling Support:

Suite Upgrade Log:

`/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.

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/postgresql_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_6.9.1c_Suite_Install_<timestamp>.log`
- `ArcSight_Logger_6.9.1c_Install_<timestamp>.log`
- `ArcSight_ESM_Manager_6.9.1c_Install_<timestamp>.log`

Prepare Resources for Upgrade

This section describes resources that the system may change during upgrade; which ones they are, and how to back them up before the upgrade so that you can copy them back after the upgrade. Standard, system-supplied resources are refreshed with new versions during upgrade. If you

customized any of these resources without copying them to another group, back them up in .arb files before you upgrade.

You do not have to restore customizations to content that is not provided by default, or to default content that you customized and put in a custom group; the upgrade does not change them.

Validate Resources

Run the resource validator (`resvalidate`) before you provide Customer Support with your system tables. Run it again after the upgrade to see if resources were rendered invalid by a change in the schema. 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 HPE ArcSight Customer Support test your upgrade will help make your upgrade run more smoothly.

Caution: As user *arcsight*, 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. Run the resource validation script as follows:

First, stop the Manager.

Run:

```
arcsight resvalidate
```

Then run:

```
arcsight resvalidate -persist false
```

Restart the Manager.

The resource validator 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 active list supplied by HPE ArcSight 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.

- It 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.
- it disables the resource so it does not try to evaluate live events in its invalid state.

Back up Resources Before Upgrade

Back up any standard content resource that you (or HPE Professional Services) modified, including active lists. Such changes are *not* preserved during the upgrade, so make a copy of them elsewhere before the upgrade begins.

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

As stated on the previous page, the upgrade does not change custom content that you put in a custom group.

To copy resources:

The objective is to separate these resources from the data that is upgraded so that it remains as is. After backing up these resources, you restore them after you have completed the entire upgrade procedure in this guide.

Perform the following operations while logged in to the ArcSight Console.

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.
3. Repeat this process for every resource type you want to back up. Any resources that point to other resources remain unchanged. That is, they still point to the other resource even if that resource was also copied. Any such pointers need to be corrected to point to the copied version.

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**.

4. 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 after upgrade

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.

The following resource configurations *are* preserved during the upgrade process, so you do not need to make a copy of them before 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

Open a Ticket with Support

Having HPE ArcSight Customer Support test your upgrade will greatly help make your upgrade run smoother. After fixing any invalid resources ("[Validate Resources](#)" on page 7), open a ticket with HPE ArcSight Customer Support to test the upgrade with your system tables and to determine if any special steps are necessary for your configuration.

Allow two weeks for ticket results when planning your upgrade.

Avoid X Windows

For Software ESM, running the upgrade in GUI mode is entirely optional. To run the upgrade in GUI mode, install the X Window system package appropriate for your operating system. Our recommendation is that you do not use X Windows and run the upgrade in console mode.

We no longer include X Windows in the operating system image provided on an appliance. When the time comes to upgrade to the new version of ESM on an appliance, you do it in console mode.

Note: In GUI mode, if you get a dialog box reporting an error or problem and the action button says **Quit**, use the **Quit** button. If you use the **X** in the upper right corner of the dialog, the process does not quit, but cannot complete successfully with the reported error.

Convert Pager Numbers to Emails

This release has discontinued support for pager notification destinations. The upgrade changes pager destinations to email. If you prefer, you can edit them before the upgrade to change the destination type to email and supply an email address. Optionally, you can wait until after the upgrade. After the upgrade, when you open what used to be a pager notification, it asks you to supply an email address.

Restore Default Manager Truststore Password

Restore your Manager Truststore to its default value of *changeit*.

When SSL Client Based Authentication is in use, the upgrade 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 after the last installation or upgrade, the certificate import does not occur. The upgrade completes, but the Manager service status shows up as "initialized" indefinitely.

Restore your secure password after the upgrade.

Use the Same File System - Software ESM

For software ESM, both XFS and EXT4 file system formats are supported during installation. However, ESM configures itself to the file system upon which it was first installed; you therefore cannot change the file system type after installation, even during an upgrade.

Set Disk Space - Software ESM

- Make sure that the amount of free space in your `/opt` directory is at least 50 GB.
- Make sure that you have at least 5 GB free disk space in your `/tmp` directory.

Set Java (Manager) Heap Size

If the Manager heap size is less than 16 GB, a message appears during the upgrade recommending that you increase the Java heap size to at least 16 GB after the upgrade is complete.

To avoid that message, change the Manager heap size in the ArcSight Command Center before you start. Refer to the *ArcSight Command Center User's Guide* for information on changing the Manager heap size.

Install the Time Zone Package - Software ESM

This is not an issue for ESM on an appliance.

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 6.7 and CentOS 6.7 use `tzdata-2014f-1.el6.noarch.rpm`.

To install it use the command:

```
rpm -Uvh <package>
```

Check to make sure that the `/etc/localtime` link is pointing to a valid time zone by running 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>
```

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 `/etc/init.d/arcsight_services tryForceStop all`
2. As user *root*, run the following command (this is one line):

```
/opt/arcsight/manager/bin/arcsight tzupdater /opt/arcsight /opt/arcsight/manager/lib/jre-tools/tzupdater
```

3. Monitor for any failure.
4. Restart all arcsight services.

Review High Availability Module Upgrade - Software ESM

The High Availability (HA) Module is a separately licensed feature.

Background:

There is a High Availability solution that was made available before ESM 6.8c (before December of 2014). Then, for ESM 6.8c there was a new High Availability product called the High Availability Module. The High Availability Module is a completely different product than the older product and there is no upgrade path from the old HA solution to the newer HA Module. The new High Availability Module uses new software and a different hardware configuration to manage failovers.

If you do not have the newer HA Module and would like to get it, purchase a license for it and install it as new, after you upgrade ESM.

Upgrading the High Availability Module 1.0 to HA 6.9.1

If you are already using the High Availability Module 1.0, which was released with ESM 6.8c, you can upgrade it to the new version.

The steps for upgrading ESM with the HA module are in the *HP ArcSight ESM High Availability Module User's Guide*. This guide lays out the steps on the primary and the secondary.

Download the Upgrade Utilities Package

The upgrade utilities package is available for download from HPE at <https://softwaresupport.hp.com/>. Download the file: `esm.utilities.{versionNum}.tgz`.

Download the upgrade file, `ArcSightESMSuite-6.9.1.xxxx.tar` from the same web site. The xxxx in the file name stands for the build number.

Copy it to the system you will be upgrading.

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

Visit the following site for information and instructions:

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

For Software ESM, if you plan to install the Risk Insight software with ESM, create a new partition with at least 25 GB for it in addition to the space allocation you make for ESM.

Consult the *ArcSight Risk Insight Deployment Guide* for details. Risk Insight is not licensed for use on an appliance.

Chapter 2: Running the Upgrade

This chapter describes the steps required to upgrade your system: There are three paths depending on what you have now:

Software ESM 6.5c SP1 or ESM 6.8c. see ["Upgrade Software ESM to ESM 6.9.1c" below](#).

ArcSight Express 4.0 patch 1, see ["Upgrade ArcSight Express to ESM Express 6.9.1c" on page 15](#).

ESM Express 6.9.0, see ["Upgrade ESM Express to ESM Express 6.9.1c" on page 22](#).

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.

If you modified any ArcSight environment variables related to ESM, restore them to what they were when you first installed ESM. There are some that, if they are altered, the upgrade may fail. If you need help, contact support.

Upgrade Software ESM to ESM 6.9.1c

To upgrade the components in your existing software ESM installation:

1. Login in as user *root*.
2. Upgrade your operating system to RHEL 6.7. You must do this before you upgrade ESM.
3. As user *arcsight*, untar the `ArcSightESMSuite-6.9.1.xxxxx.tar` file:

```
tar xvf ArcSightESMSuite-6.9.1.xxxxx.tar
```

4. As user *root*, remove services before running the upgrade. Run
`cd <untar directory>/Tools`
`./stop_services.sh`
 The Tools folder is wherever you untarred the file.

5. Provide execute permission to `ArcSightESMSuite.bin` file:

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

6. As user *arcsight*, run the upgrade:

```
./ArcSightESMSuite.bin -i console
```

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.

7. It asks you to confirm that you want to upgrade your existing ESM installation. type **Yes** and press

Enter.

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

If you get a Java (Manager) Heap Size error message, you may click OK to continue. You will need to change the Manager Heap Size to at least 16 GB after the upgrade. Refer to the *ArcSight Command Center User's Guide* for information on changing the Manager heap size.

If the upgrade fails, check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file to see where it 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:

```
Pre-upgrade tasks completed successfully.
```

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

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.

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

8. Read through the Introduction screen and press **Enter**.
9. Press **Enter** to scroll to through the license agreement then select "I accept the terms of the License Agreement" and press **Enter**.
10. Press **Enter** to scroll to through the notice and press **Enter**.
11. Specify or select where you would like the link for the installation to be created and press **Enter**.
12. Review the settings and select **Install** and press **Enter**.

13. The upgrade reports when all components have been copied over. Press **Enter**.

The upgrade transfers configurations, upgrades the schema, and upgrades the content.

14. The upgrade shows you the progress as the components get installed and reports **Upgrade Complete** when the upgrade is finished.

15. As user *root*, run this script to set up arcsight services:

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

16. Follow applicable post-upgrade steps listed in the section, ["Post Upgrade Tasks" on page 24](#).

Handling a Missing Time Zone Updater

The upgrade gives you a message if it cannot find the time zone information for the ESM components. There are two reasons why you might get this message:

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 time zone info for the ESM components after the upgrade. Refer to ["Install Time Zone Package - Software ESM" on page 25](#), to correct either of these time zone issues.

Upgrade ArcSight Express to ESM Express 6.9.1c

When upgrading from ArcSight Express 4.0, patch 1, there are several steps:

- If you installed the ArcSight Express security update of January 7, 2016, uninstall it. (This is the security update that fixes NGS-15050.) Do not uninstall patch 1.

Caution: If you do not remove this update, `uninstall_conapp.sh`, `uninstall_connectors.sh`, and `ArcSightESMSuite.bin` do not run correctly.

To remove the update, follow the uninstall instructions in the documentation that came with the security update.

- Migrate the Connector Appliance application to a new ArcSight Management Center on another machine. This procedure has several substeps of its own, including downloading its own scripts and manually saving and copying files.
- Upgrade the appliance operating system.

- Download and untar the Upgrade file.
- Upgrade ArcSight Express.

This section takes you through all these steps in the required order.

Migrate Connector Appliance and Connector Data to ArcSight Management Center – ArcSight Express Only

Uninstall the security update of January 7, 2016 that fixes bug NGS-15050. It secures certain Connector Appliance files in a way that prevents the upgrade from removing them. Instructions are in the documentation that came with the security update. (Do not uninstall Patch 1.)

If you do not use the Connector Appliance for remote management of connectors on ArcSight Express, you may skip the rest of this section. (You still have to uninstall the security update, because the affected files are there whether you use ConnApp or not.) Go to "[Delete Unneeded ArcSight Express Directories](#)" on page 18.

As part of your upgrade to ESM Express 6.9.1, you migrate your Connector Appliance and remote connector data (if any) to a software ArcSight Management Center 2.1, which will manage such data going forward. The Connector Appliance module in ArcSight Express is no longer supported in ESM Express 6.9.1 and later versions.

ArcSight Management Center (ArcMC) is the successor product to Connector Appliance, which includes all the functionality of Connector Appliance and much more. You can retain all of your existing Connector Appliance data and simply migrate the data to the new ArcSight Management Center software platform. However, unlike Connector Appliance, your new software ArcMC runs on a separate host from your ESM Express. Your ArcSight Management Center will then manage remote connectors on the ESM Express.

Before Performing the Migration

Before performing your Connector Appliance and connector data migration from ArcSight Express, do each of the following.

1. Download and review the ArcSight Management Center 2.1 Administrator's Guide, available from the HP ESM community at [Protect724](#). The guide explains the management and administration of ArcSight Management Center in detail.
2. Also from [Protect724](#), download and review the ArcSight Management Center 2.1 Release Notes to get system requirements for installation. Ensure your new ArcSight Management Center host meets these requirements.
3. Download the ArcSight Management Center 2.1 software from the HPE SSO download site.
4. Prepare a secure, appropriate, and technically sufficient host for running the ArcSight Management Center software. Then follow the instructions in the ArcSight Management Center Administrator's Guide and Release Notes to install ArcSight Management Center 2.1 on the host.

5. Download and store the migration scripts tar file `esm.utilities.<timestamp>.tgz` in a secure network location. This tar file contains the scripts needed for data migration.

The Data Migration Process

The data migration process comprises these tasks:

1. Back up all of your Connector Appliance and connector data on your existing ArcSight Express.
2. Copy the backup to your new ArcSight Management Center system, and then restore your backed-up data to the new ArcSight Management Center system.
3. Delete the unneeded directories from ArcSight Express.

Each of these tasks is explained in detail below.

Backing Up Your Connector Appliance and Connector Data on ArcSight Express.

To back up your Connector Appliance and connector data on ArcSight Express:

1. In ArcSight Express, browse to **Repositories > Backup Files > Retrieve Container Files**.
2. Choose *Local Connectors*. This saves your connector data in the repositories folder.
3. SSH to ArcSight Express and log in as user `arcsight`.
4. Copy the tar file `esm.utilities.<timestamp>.tgz` to the `/home/arcsight` directory on your ArcSight Express.
5. Untar the file as follows: `tar -xzf esm.utilities.<timestamp>.tgz`

The `untar` command for the `esm.utilities.<timestamp>.tgz` file creates the `esm.utilities/express` folder in the location where you untar it. In this case, `/home/arcsight/esm.utilities/express`.

6. Run the backup script to back up your Connector Appliance and connectors data:
`./home/arcsight/esm.utilities/express/conapp_connectors_zip.data.sh <dir>`

`<dir>` is the full path to a directory to which the user `arcsight` has write permissions. Your backed up data will be in a file called `DataBackupConappFromAE.tar.gz`.

Restoring Your Connector Appliance and Connector Data to ArcMC

After installation of the ArcSight Management Center 2.1 software, you are now ready to run the restore script on your new ArcMC. Before continuing, note the following:

- You must run the script using the same user account that was used to install ArcSight Management Center
- Ensure that the XSLT proc libraries exist in the directory where ArcSight Management Center is installed. (These are an included part of the OS of the system hosting your ArcSight Management Center).

To run the restore script on ArcMC:

1. Copy the DataBackupConappFromAE.tar.gz file containing your connector data, as well as the tar file containing the scripts; esm.utilities.<timestamp>.tgz.
2. Log in to ArcMC with the same user account used to install ArcSight Management Center.
3. Untar the file as follows:

```
tar -xzf esm.utilities.<timestamp>.tgz
```

 This creates the esm.utilities folder.
4. In the esm.utilities\express subfolder, enter:

```
chmod +x conapp_to_arcmc_migration.sh
```
5. Run the script:

```
./conapp_to_arcmc_migration.sh <ArcMC_installdir> <backup_path>
```

, where
 - <ArcMC_installdir> is the absolute path of the installation directory for ArcMC
 - <backup_path> is the absolute path of the DataBackupConappFromAE.tar.gz file containing your backed-up data

The script unzips the DataBackupConappFromAE.tar.gz file, stops the web process, adds the remote configuration into ArcSight Management Center ArcSight Management Center, and restarts the web process. The install process is logged to <ArcMC_install directory>/userdata/logs/arcmc/AEConappToArcMCMigration.log.

Verify that ArcSight Management Center is up and running before proceeding with the rest of your ArcSight Express upgrade.

Note: In ArcMC, on the **Containers** tab, in the **Issues** column, the localhost will show *Unknown Issue* because the host will not be accessible.

Delete Unneeded ArcSight Express Directories

For ArcSight Express users, after you have completed the data migration to ArcSight Management Center and you have verified the correct operation of ArcMC, you can delete your unneeded directories from ArcSight Express and reclaim the disk space. The scripts here are included in the tar file you untarred in the previous topic.

To delete unneeded directories from ArcSight Express:

1. Login in as user *root*.
2. The untar command for the `ArcSightESMSuite-6.9.1.xxxxx.tar` file created the `Tools` folder in the location where you untarred it. Change to that directory. For example:
`cd /home/arcsight/esm691/Tools.`
3. Remove services before running the upgrade. From the `Tools` folder, run:
`./stop_services.sh`
4. Log into ArcSight Express as user *arcsight*.
5. The untar command for the `esm.utilities.<timestamp>.tgz` file created the `esm.utilities/express` folder in the location where you untarred it. Change to that directory. For example:
`cd /home/arcsight/esm.utilities/express.`
6. From the `esm.utilities/express` folder, run:
`./uninstall_conapp.sh`
 This uninstalls and deletes the `conapp` directory.
7. Log in as user *root*.
8. From the `esm.utilities/express` folder, run:
`./uninstall_connectors.sh`
 This removes the `connector_1` and `connector_2` directories (local onboard connectors).

For troubleshooting purposes, log files of the above scripts are located as follows:

Script	Log Location
<code>uninstall_conapp.sh.</code>	Same location as scripts, in the log file <code>UninstallConapp.log</code> . For example, <code>home/arcsight/esm.utilities/express/UninstallConapp.log</code>
<code>uninstall_connectors.sh.</code>	<code>/opt/arcsight/UninstallConnectors.log</code>
<code>connapp_connectors_zip_data.sh</code>	Same directory as backup directory, in the file <code>Conapp6_4_P2/DataBackupConappFromAE.log</code>

Upgrade the AE Operating System

This section provides information on how to upgrade from RHEL 6.x to RHEL 6.7 on an ArcSight Express 4.0 Patch 1 appliance. Perform this upgrade *before* you upgrade your ArcSight Express installation to ESM Express 6.9.1.

1. As user *root*, download the upgrade file to any folder. The file is:
`ae-rhel67upgrade.tar.gz`

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

Visit the following site for information and instructions:

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

2. From the directory where you downloaded the archive in step 1, extract it as follows:
`/bin/tar zxvf ae-rhel67upgrade.tar.gz`

3. Change directory:
`cd ae-rhel67upgrade`

4. Run the following command to start the OS upgrade:
`./osupgrade.sh`

This script will only run on the B7500 appliance.

You do not need to reboot the system, the script reboots it automatically after the script completes.

5. Make sure that the kernel version is `kernel-2.6.32-573.12.1.el6.x86_64`.
6. Check the operating system version by running the following command: `cat /etc/redhat-release`

The result of this command should be:

```
Red Hat Enterprise Linux Server release 6.7
```

The upgrade to RHEL 6.7 is now complete.

Upgrade ArcSight Express to ESM Express

1. If you haven't already, uninstall the ArcSight Express security update of January 7, 2016. It secures certain files in a way that prevents the upgrade from removing them. Instructions are in the documentation that came with the security update.
2. Log in as user *arcsight*.
3. You can perform the rest of the steps either directly on the machine or remotely using ssh. To use ssh, open a shell window by running:
`ssh root@<hostname>.<domain>`
4. Change to the directory where you downloaded the upgrade files.
5. Untar the `ArcSightESMSuite-6.9.1.xxxxx.tar` file:

```
tar xvf ArcSightESMSuite-6.9.1.xxxx.tar
```

6. Provide execute permission to ArcSightESMSuite.bin file:

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

7. Run the upgrade file with the following command:

```
./ArcSightESMSuite.bin -i console
```

8. Press **Enter** at the following prompt to accept the default, which is Yes:

```
Do you want to upgrade your existing installation to version 6.9.1c?
```

9. 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.

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

Before the upgrade process begins, the existing software components will be backed up into the following location:

- /opt/arcsight/manager.preUpgradeBackup
- /opt/arcsight/web.preUpgradeBackup
- /opt/arcsight/logger/BLxxxx

The system tables are exported into /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql.<timestamp>.

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

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

If you get a Java (Manager) Heap Size error message, you may click OK to continue. You will need to change the Manager Heap Size to at least 16 GB after the upgrade. Refer to the *ArcSight Command Center User's Guide* for information on changing the Manager heap size.

If the upgrade fails, check the /opt/arcsight/upgradelogs/suite_upgrade.log file to see where it 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:

```
Pre-upgrade tasks completed successfully.
```

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

After the Manager upgrade completes, the upgrade summary page opens. It may take some time for the upgrade successful message to appear in the command prompt.

As user *root*, run this script to set up arcsight services:

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

Be sure to follow applicable post-upgrade steps listed in the section, "[Post Upgrade Tasks](#)" on page 24.

Upgrade ESM Express to ESM Express 6.9.1c

If you are on ESM Express 6.9.0c, you are already on RHEL 7.1 and you do not need to upgrade the operating system.

1. Log in as user *arcsight*.
2. You can perform the rest of the steps either directly on the machine or remotely using ssh. To use ssh, open a shell window by running:

```
ssh root@<hostname>.<domain>
```

3. Change to the directory where you downloaded the upgrade files.

4. Untar the ArcSightESMSuite-6.9.1.xxxxx.tar file:

```
tar xvf ArcSightESMSuite-6.9.1.xxxxx.tar
```

5. As user *root*, remove services before running the upgrade. Run

```
cd <untar directory>/Tools
```

```
./stop_services.sh
```

The Tools folder is in the directory where you untarred the file.

6. Provide execute permission to ArcSightESMSuite.bin file:

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

7. As user *arcsight*, run the upgrade file with the following command:

```
./ArcSightESMSuite.bin -i console
```

8. Enter Y at the following prompt:

```
Note: You are about to run this product updater.
```

```
Proceed [Y/N]?
```

9. 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.

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

Before the upgrade process begins, the existing software components will be backed up into the following location:

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

The system tables are exported into `/opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql.<timestamp>`

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

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

If you get a Java (Manager) Heap Size error message, you may click OK to continue. You will need to change the Manager Heap Size to at least 16 GB after the upgrade. Refer to the *ArcSight Command Center User's Guide* for information on changing the Manager heap size.

If the upgrade fails, check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file to see where it 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:

```
Pre-upgrade tasks completed successfully.
```

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

After the Manager upgrade completes, the upgrade summary page opens. It may take some time for the upgrade successful message to appear in the command prompt.

As user `root`, run this script to set up arcsight services:

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

Be sure to follow applicable post-upgrade steps listed in the section, "[Post Upgrade Tasks](#)" on the next page.

Confirm that the Upgrade Succeeded

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`. You can view this file in a text editor or move it to a machine with a graphical user interface and a browser.

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

```
Upgrade completed successfully.
```

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:

Build versions:

```
esm:6.9.1.xxxxx.x(BExxxxx)
storage:6.9.1.sssss.s(BLsssss)
process management:6.9.1-mmmmm
installer:6.9.1-iiii
```

```
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
```

The build versions of the components are another good way to verify a successful upgrade:

Run the following command to check the RPM versions:

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

You have upgraded to ESM 6.9.1c.

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

Make sure to upgrade your existing Console. See ["Upgrading ArcSight Console" on page 29](#).

Manager Initializing Indefinitely

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).
`/etc/init.d/arcsight_services stop manager`
2. From the `/opt/arcsight/manager/bin` directory, run the following command:

```
./arcsight keytool -store managercerts -importcert -alias services_admin -file
/opt/arcsight/manager/config/service-certificate.cer -noprompt
```
3. Restart the Manager.
`/etc/init.d/arcsight_services start manager`

Post Upgrade Tasks

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

Install Time Zone Package - Software ESM

If you complete the upgrade without installing the time zone update, you can set up the time zone package at any time after the upgrade. Use the following procedure after ensuring that you have downloaded and installed the correct package and the link is set correctly.

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/arcsight/manager/lib/jre-tools/tzupdater
```

3. Monitor for any failure.
4. Restart all arcsight services.

Fix Invalid Resources

You checked for invalid resources before the upgrade and you do it again here to find any that were rendered invalid by the upgrade.

The resource validator 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 HP 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.

- It 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.
- It disables the resource so it does not try to evaluate live events in its invalid state.

Install Netflow SmartConnectors

The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors, which are not installed with ESM 6.9.1c.

- ArcSight IP Flow SmartConnector
- ArcSight QoSient ARGUS SmartConnector

To use the NetFlow Monitoring content, install and configure these SmartConnectors. For information about how to obtain the SmartConnectors, contact your HPE ArcSight sales representative.

Supply Email Addresses for Converted Pager Destinations

This release has converted pager notification destinations to email. If you did not do this before the upgrade, edit them now to supply an email address.

Delete Unassigned File Resources

The upgrade might result in unassigned resources. For example, the .art files are created as new file resources in ESM 6.9.1c, and the resources get new version IDs during the upgrade. The original files are stored in the Files resource under the Unassigned folder.

You can safely delete the unassigned .art files after an upgrade because they are duplicates.

Restore Deprecated Resources

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 still plan to use this deprecated resource after the upgrade, move it to your own group after upgrading.

Restore Custom Velocity Templates

The upgrade preserves customized velocity templates by adding the .previous file extension and replacing 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`.

Restore Custom Case UI

If you customized the Cases UI on the existing 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 after the upgrade; some are not. Restore them manually after the upgrade as follows:

1. 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.

2. After copying the customized files to the Manager, copy the following files to the individual Console installations at `arcsight\console\i18n\common\`:
 - `label_strings`
 - `resource_strings`
3. Copy `caseui.xml` under `/opt/arcsight/manager.preUpgradeBackup/config` to `/opt/arcsight/manager/config`.
4. 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`.
5. Restart the Manager for these changes to take effect.

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

Verify and Reapply Configurations

Verify and restore standard content after the upgrade.

1. Verify that your configured resources that you did not back up retained their configurations as expected. A list of resources that you did not have to back up is in the topic ["Prepare Resources for Upgrade" on page 6](#)
2. Reconfigure the resources that require restoration.

- a. Re-import the package you created in the topic ["Prepare Resources for Upgrade" on page 6](#)
- 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.

Verify 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. See ["Fix Invalid Resources" on page 25](#).

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 file name represents the Console build number:
 - ArcSight-6.9.1.xxxx.0-Console-Win.exe
 - ArcSight-6.9.1.xxxx.0-Console-Linux.bin
 - ArcSight-6.9.1.xxxx.0-Console-MacOSX.zip
3. If you downloaded the 6.9.1c Console installation file to a different machine, transfer it to the machine on which you plan to install the Console.

Run the ESM 6.9.1c Console Installation

1. Run the installation file appropriate for your platform:
 - **On Windows:**
Double-click ArcSight-6.9.1.xxxx.0-Console-Win.exe

- **On Macintosh:**

Unzip the following file:

ArcSight-6.9.1.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-6.9.1.xxxx.0-Console-Linux.bin

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

```
./ArcSight-6.9.1.xxxx.0-Console-Linux.bin -i console
```

Step through the Installation wizard screens. 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 6.9.1 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.

2. 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**.
3. You are 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**.

Run the ESM 6.9.1c Console Configuration

See the ESM Installation and Configuration Guide for details on the remaining screens for installing a Console using the installation wizard. Look in the section "Configuring the ArcSight Console," which is in chapter 3, "Installing ArcSight Console."

Start the ArcSight Console.

Post-Console-Upgrade Tasks

After you have upgraded a Console to 6.9.1c check to make sure that:

1. You can view the upgraded standard content.
2. All your SmartConnectors are connecting to the Manager on the ESM system.
3. 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 6.9.1c structures. Manually fix any content that migrated to an unwanted location, or whose conditions are no longer valid.

Note: After the upgrade, the only packages that are installed are those that were installed before the upgrade. That means that, even if a new package is mandatory, the upgrade imports it, but you have to install it manually in a separate operation.

- **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.

Note: HPE 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.
- **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 upgrade to ESM 6.9.1c. This may happen for assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In 6.9.1c, 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 6.9.1c. 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 6.9.1c 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 6.9.1c, 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.
- Depreciated 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 6.9.1c 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: HPE no longer supports deprecated resources, so if you choose to restore a deprecated resource, you are responsible for its maintenance.

HPE also recommends that you verify whether the new 6.9.1c resources address the same goal more efficiently.

After upgrading, 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

Note: HPE 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.

Upgrade 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 6.9.1c

This chapter describes the method for upgrading a multi-ESM deployment to 6.9.1c.

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 ["Running the Upgrade" on page 13](#) to upgrade your ESM to 6.9.1c.
4. Once ESM 6.9.1c is running, follow instructions in the ["Upgrading ArcSight Console" on page 29](#) to upgrade any Consoles connected to it.
5. Upgrade the Forwarding Connector connected to this ESM to the version specified in the Support Matrix for this ESM release.

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.

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 6.9.1c)

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@hpe.com.

We appreciate your feedback!