Micro Focus Security ArcSight ESM

Software Version: 7.0 Patch 1

Upgrade Guide

Document Release Date: August 16, 2018
Software Release Date: August 16, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Chapter 1: Preparing for the Upgrade

This document describes the steps required to upgrade software ESM or ESM on an appliance to version 7.0 Patch 1. This section includes a summary and some essential prerequisites.

Terminology to Note

ESM Appliance and **ESM Express** are different licensing models installed on an appliance.

Software ESM is ESM installed on your own hardware.

The supported upgrade paths are:

- 6.11.0 (with the latest patch is recommended). You must first upgrade the operating system to RHEL 6.9, RHEL 7.4, CentOS 6.9, or CentOS 7.4.
- From ESM 6.11.0 on an appliance to ESM 7.0 Patch 1 with RHEL 7.4 on the B7600 appliance.

For details on supported platforms, refer to the *ESM Support Matrix* available on Protect 724.

Note: If you want to run ESM in distributed correlation mode, complete the upgrade to ESM 7.0 Patch 1 as directed in this guide, and then convert the system to distributed correlation mode. To perform this conversion, see "Converting Compact Mode to Distributed Correlation Mode - Optional" on page 21. Conversion to distributed correlation mode is not supported on the Appliance.

Verify Proper Operation

Verify that your existing ESM on an appliance or software ESM is fully functional and that its archives are intact. If there is any issue with your existing system, contact Customer Support before upgrading.

In Case of Upgrade Problems

Caution: After you start the upgrade, you cannot roll back to the previous version. Do not attempt to use the Uninstall link to roll back the upgrade, as it will not work. If you encounter errors when upgrading, contact Customer Support for help to move forward with the upgrade process.

Have the system tables available when calling Customer 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:

- `/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

Manager Upgrade Logs:

The log files are located in the `/opt/arcsight/var/logs/misc/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 run it. Make sure to use the right one. The directory for the timestamp log folder is `/opt/arcsight/manager/upgrade/out/18-07-31_10-21-29`.

ArcSight Services Upgrade Logs:

The log file `arcsight_services.log` is located in the `/opt/arcsight/services/logs` directory, and contains information about starting and stopping services during upgrade.

Installation Logs

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

- `ArcSight_ESM_*.log`
- `ArcSight_Logger_*.log`
- `ArcSight_ESM_Manager*.log`

Make a Copy of /opt/arcsight

Before starting the upgrade, either make a copy of `/opt/arcsight` (with the exception of the `/opt/arcsight/logger/data` directory) or follow the CORR-E Backup and Recovery guide instructions to create a backup copy of the system.

Prepare Resources for Upgrade

This section describes resources that the upgrade does or does not change.

Caution: Beginning with ESM 7.0 Patch 1, the Event Reconciliation and Session Reconciliation data monitors are deprecated and therefore no longer functional. If you customized these data monitors and apply the upgrade, the customized DMs will be invalid (will appear as broken resources).

Standard, ESM-supplied resources:

These are refreshed with new versions during upgrade.

- If you customized any of these resources by copying them into a custom group, be aware that the custom group is not affected by the upgrade.
- If you have to customize resources from their original location, back them up in an `.arb` file (make sure to exclude any other related resources) before upgrade. You can restore them after the upgrade.
- When you restore an .arb file, it overwrites the version that the upgrade places there, so if the upgrade offered any improvements, they will be lost. An option is to apply your customizations to the new version.

Customizations that are not affected:

There are changes to certain resources that you can make without making another copy and the upgrade does not overwrite these customizations:

- 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
  - Custom network resources
  - Custom location resources
- SmartConnectors
- Users and user groups
- Report schedules
- Archived reports
- Notification destinations and priority settings
- Cases

Customizations to the Cases Editor user interface:

If you customized the Cases Editor user interface, back up the customized files in a separate location and restore them after the upgrade.

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 "Fix Invalid Resources" on page 24 for details. 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.

1. Stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. As user *arcsight*, run:

   ```
   ./arcsight resvalidate -persist false
   ```

   When you run `resvalidate` these two different ways, two files (`validationReport.html` and `validationReport.xml`) are generated in the same directory. Save these files to another directory so you can compare them to the same files generated after the upgrade.

3. Restart the Manager:

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

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, for example:

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

You run this again after the upgrade.

Back Up Resources Before Upgrade

Back up any standard content resource that you (or 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 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 back up resources:

Separate these resources from the data that is upgraded, and then back up these resources. You restore them after you have completed the entire upgrade procedure.

1. While logged in to the ArcSight Console, for each resource type (filter, rule, active list), create a new group under your personal group. Provide a name that identifies the contents.
2. Right-click your group name and select **New Group**.
3. Copy the resources into the new group.
4. Repeat steps 1 through 3 for each 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**.
5. Export the backup groups in a package.
   a. 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.
   b. Select the group that you created in step 1, right click and select **Add to Package**. Select your new package and click **OK**.
   c. 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 resource configurations that *are* preserved during the upgrade process are listed in "Customizations that are not affected:" on page 7. You do not need to make a copy of them before the upgrade.

Test Your Upgrade

It is strongly recommended that you test your upgrade before upgrading your production environment. The steps in this topic contain an example of how to perform this test.

An example upgrade test:

1. Install ESM in a test environment that matches your current production environment as closely as possible, including:
   - The ESM version and patch must be the same.
   - The system (physical or virtual) must have sufficient memory and processing power to start all ESM services (16GB RAM or greater is recommended).
   - Ensure that the newly installed test version of ESM starts and works correctly **before** importing the test system tables.
   - This is a system tables test only, so you do not need to configure LDAP, SMTP server of CA certificates.
2. Stop the Manager in the production environment.

   `/etc/init.d/arcsight_services stop manager`
3. Export the system tables from the production environment.

   ```
   cd /opt/arcsight/manager/bin
   ./arcsight export_system_tables arcsight <mysql password> arcsight -s
   ```
4. Start the Manager in the production environment.
5. `/etc/init.d/arcsight_services start all`
6. Move the system tables dump to the test environment under `/opt/arcsight/manager/tmp`.
7. Stop the Manager in the test environment.

   `/etc/init.d/arcsight_services stop manager`
8. Import the system tables from the production environment into the test environment.

   ```
   cd /opt/arcsight/manager/bin
   ./arcsight import_system_tables arcsight <mysql password> arcsight
   <system-table-dump filename>
   ```
9. Start the Manager in the test environment.

   `/etc/init.d/arcsight_services start manager`
10. Verify that the Manager in the test environment is functioning after the import of the system tables from the production environment. Ensure that the test Manager is completely up and running.
11. Stop the Manager in the test environment.

    `/etc/init.d/arcsight_services stop manager`

    Verify that the test system is completely down.
12. Run `resvalidate` to validate resources. See "Validate Resources" on page 8 for details.
13. Proceed with the upgrade procedure in the test environment, beginning with Chapter 1 in this guide, "Preparing for the Upgrade" on page 5.

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.

X Windows is not included in the operating system image provided on a G9 appliance. When the time comes to upgrade to the new version of ESM on an appliance, perform the upgrade 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. Using the **X** in the upper right corner of the dialog is not recommended.

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.

Restore Default Console Truststore Password

Trusted certificates from the previous truststore cannot be transferred to the new truststore without setting the password back to the default value. You **must** restore your Console Truststore to its default value of `changeit`. If you do not change the password to the default value, the Console upgrade will fail. After the settings have been transferred, you can change the password of the new truststore.

Do Not Change the 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

It is recommended that you change the Java heap size to at least 16 GB before you begin the upgrade. If the Manager heap size is less than 16 GB, a message during the upgrade recommends that you increase the Java heap size to at least 16 GB after the upgrade is complete.

To avoid that message, change the Manager Java heap size before you start. As user *arcsight*, run `/opt/arcsight/manager/bin/arcsight managersetup` to increase the Java heap size. See the *ArcSight ESM Administrator's Guide* for details on running `managersetup`.

Install the Time Zone Package - Software ESM

This section does not apply to 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. It is recommended to install the time zone update package before the upgrade.

For RHEL 7.4 and CentOS 7.4 use `tzdata-2018c-1.el7.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>
```

Note: If the `/etc/localtime` link is not pointing to a valid time zone, the ESM installation stops. In this case, you must manually set the link to a valid timezone.

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

If you complete the installation without the required tzdata rpm package, 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 tzdata package and the link `/etc/localtime` is set correctly. The following steps must be completed after the upgrade:

1. As user *arcsight*, shut down all arcsight services. This is an important step. Run:
   ```
   /etc/init.d/arcsight_services stop all
   ```
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:
   ```
   /etc/init.d/arcsight_services start all
   ```

Review High Availability (HA) Module Upgrade - Software ESM

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

Note: A High Availability solution was available **before** ESM 6.8c (before December of 2014). As of ESM 6.8c, the HA Module was provided. The HA Module is a completely different product than the High Availability product that existed before ESM 6.8c. There is no upgrade path from the pre-6.8c High Availablity solution to the newer HA Module.

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

If you are already using the HA Module, you can upgrade it to the new version. The steps for upgrading ESM with the HA module are in the *ESM High Availability Module User's Guide*. This guide describes the steps on the primary and the secondary.

Download the Upgrade Package

Download the upgrade file, `ArcSightESMSuite-7.0.0.xxxx.1.tar` from https://softwaresupport.softwaregrp.com/. The xxxx in the file name stands for the build number. Copy the file to the system you will be upgrading.

After you download the software, contact support to verify that the signed software you received is indeed from Micro Focus and has not been manipulated by a third party.

Chapter 2: Running the Upgrade

This chapter describes the steps required to upgrade your system from software ESM 6.11.0 or from ESM 6.11.0 on an appliance.

Upgrade Software ESM

Note: If you are upgrading a High Availability (HA) implementation, note that HA is supported only on the persistor node in the distributed correlation cluster. HA is not supported on any non-persistor node in a distributed correlation cluster.

To upgrade the components in your existing software ESM installation:

1. Login in as user *root*.
2. Stop all services:

   ```
   /etc/init.d/arcsight_services stop all
   ```
3. Upgrade your operating system to the supported operating system version. Refer to the ESM Support Matrix. You must do this before you upgrade ESM.
4. Services will restart after you complete the operating system upgrade and reboot the system. Verify that all services start and are available before continuing with the upgrade.
5. As user *arcsight*, untar the `ArcSightESMSuite-7.0.0.xxxx.1.tar` file:
   `tar xvf ArcSightESMSuite-7.0.0.xxxx.1.tar`
6. 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.
7. 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.
8. It asks you to confirm that you want to upgrade your existing ESM installation. Type **Yes** and press **Enter**.

   If you get a Java (Manager) Heap Size error message, press **Enter** to continue. You will need to change the Manager Heap Size to at least 16 GB after the upgrade. See "Set Java (Manager) Heap

Size" on page 12 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 fails at any point after the pre-upgrade tasks, contact ArcSight Customer Support for help with recovering from the failure and send all files in these directories:

`/opt/arcsight/upgradelogs/`

`/opt/arcsight/logger/current/arcsight/logger/logs/`

`/opt/arcsight/var/logs/misc/upgrade/`

to Customer Support.

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.

Contact Customer Support if you need assistance.

9. Read through the Introduction screen and press **Enter**.
10. Press **Enter** to scroll to through the license agreement the message DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N) displays. Type **Y** and **Enter**.
11. Press **Enter** to scroll to through the notice and press **Enter**.
12. Specify or select where you would like the link for the installation to be created and press **Enter**.
13. Review the settings and select **Install** and press **Enter**.
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 21.

Handling a Missing Time Zone Updater

The upgrade gives you a message if it cannot find the time zone information for the ESM components. This can occur if a timezone version 2017c or later rpm for your operating system is not installed.

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 23, to correct either of these time zone issues.

Upgrade ESM on an Appliance

Upgrade the Operating System

If you are on ESM 6.11.0 on an appliance, and you are using RHEL 6.8, you must upgrade the operating system to RHEL 6.9.

To Upgrade from RHEL 6.8 to RHEL 6.9

1. As user *root*, download the upgrade file to any folder. For RHEL 6.9, this file is: `esm-rhel69upgrade.tar.gz`.

   After you download the software, contact support to verify that the signed software you received is indeed from Micro Focus and has not been manipulated by a third party.
2. From the directory where you downloaded the archive in step 1, extract it as follows for RHEL 6.9:
   `/bin/tar zxvf esm-rhel69upgrade.tar.gz`
3. Change directory:
   cd `esm-rhel69upgrade`
4. Run the following command to start the operating system upgrade and generate an upgrade log file:
   `(./osupgrade 2>&1) | tee /tmp/osupgrade.log`
   The system reboots after the operating system upgrade completes.
5. Check the operating system version by running the command:

   `cat /etc/redhat-release`

   The result of this command should be:

   `Red Hat Enterprise Linux Server release 6.9`

   The upgrade to RHEL 6.9 is now complete.
6. The system reboots automatically; services will restart after the operating system upgrade is complete. Verify that all services start and are available before continuing with the upgrade.

ESM on an Appliance Upgrade

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-7.0.0.xxxx.1.tar` file:

   ```
   tar xvf ArcSightESMSuite-7.0.0.xxxx.1.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. As user *arcsight*, run the upgrade file with the following command:
   ```
   ./ArcSightESMSuite.bin -i console
   ```
7. 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`

   Services are backed up to `services.preUpgradeBackup`. The suite is backed up to `suite.preUpgradeBackup`. The system tables are exported into `/opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql.<timestamp>`.

   Do not delete the backup files before the upgrade is completely done and verified to be successful. You might need them to recover the system 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 press **Enter** to continue. You will need to change the Manager Heap Size to at least 16 GB after the upgrade. See "Set Java (Manager) Heap Size" on page 12 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 Micro Focus ArcSight Customer Support for help with recovering from the failure and send all the `/opt/arcsight/upgradelogs/*` to them.

After the Manager upgrade completes, go to the following location and check the upgrade summary report: `/opt/arcsight/manager/upgrade/out/16-09-08_16-06-55/summary.html`

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 21.

Convert the Appliance to Prefer IPv6 - Optional

After the upgrade, you can convert your ESM appliance to use IPv6. This is an optional procedure, and the purpose of it is to convert the appliance to a pure IPv6 network configuration and convert ESM to prefer using IPv6, or to convert the appliance to a dual stack configuration.

Note that any connectors registered on the appliance will need to be re-registered after you perform this conversion because the IPv4 IP address will change to a hostname, and the Manager certificate will be regenerated.

After the upgrade, convert your appliance to IPv6 using this procedure:

1. Stop all the services. As user *root* or *arcsight*, run:
   `/etc/init.d/arcsight_services stop all`
2. Confirm if all services are stopped. As user *root* or *arcsight*, run:
   `/etc/init.d/arcsight_services status all`
3. As user *root*, run the network configuration script to change the operating system by selecting IPv6 or Dual Stack:
   `/opt/arcsight/services/bin/scripts/nw_reconfig.py`
4. Reboot the system.
5. As user *root*, edit the `/etc/hosts` file and comment out the line that contains an IPv4 address to a hostname mapping, if present.
6. Stop the Manager service. As user *root* , run:
   `/etc/init.d/arcsight_services stop manager`
7. Re-run managersetup. As user *arcsight* , run:
   `/opt/arcsight/manager/bin/arcsight managersetup`

   Change the preferred IP protocol to IPv6 and change the hostname to the hostname of the appliance's IPv6 address.

   Regenerate the Manager certificate.
8. Start the Manager. As user *root* , run:
   `/etc/init.d/arcsight_services start all`
   ESM now uses IPv6.

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 this file: `<ARCSIGHT_HOME>/upgrade/out/<timestamp>/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.
```

Note: You may see a message like: `Could not convert table(s) arc_ald_xxxxxx, arc_ald_yyyyyy without column details in arc_db_table_schema.` in the `/opt/arcsight/manager/upgrade/out/<timestamp>/logs/upgrade/server.upgrade.log` file. This message indicates some existing tables were not upgraded due to missing some meta data. Tables without meta data are probably no longer used and this condition should not affect existing functionality.

Check the build versions by running the following command:

```
/etc/init.d/arcsight_services version
```

You should see a response similar to the following:

```
Build versions:
     esm: 7.0.0.2436.1(BE2436)
     storage: 7.0.0.1965.1(BL1965)
     process management:7.0.0-2234
     installer:7.0.0-2234
```

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
```

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

Run the following command to check the RPM versions:

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

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 46.

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. Start the Manager.
   `/etc/init.d/arcsight_services start all`

Chapter 3: Post Upgrade Tasks

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

Converting Compact Mode to Distributed Correlation Mode - Optional

This topic applies only if you are converting your system from compact mode to distributed correlation mode. If you do not want to perform such a conversion, you can skip the tasks in this topic.

If you have ESM installed in compact mode, you can later convert the system to distributed correlation mode. You can convert a new install of ESM, or can convert a system that has been upgraded to the latest ESM version.

It is important to plan the cluster before you being cluster implementation. Before performing this procedure, see "Distributed Correlation Cluster Planning" in the *ESM Installation Guide* for details.

To convert your system from compact mode to distributed correlation mode:

1. Verify that all services are running:

   `/etc/init.d/arcsight_services status`
2. Change the user to *arcsight*:

   `su - arcsight`
3. Stop the Manager:

   `/etc/init.d/arcsight_services stop manager`
4. Change directory to `/opt/arcsight/manager`:

   `cd /opt/arcsight/manager`
5. Initialize distributed correlation mode:

   `bin/arcsight initialize-distributed-mode`
6. Setup the repository, using the option **Change the TCP Port Range for ESM Processes** to set up the port range:

   `bin/arcsight reposetup`

   See "Configuring a Repository" in the *ESM Administrator's Guide* for details on running `reposetup`.
7. Run `managersetup`.

   `bin/arcsight managersetup`

Run `managersetup` . Do not change any configuration settings. Step through the wizard and allow it to save settings. Verify that you see the message "The ArcSight Manager settings have been applied." This is necessary even though no settings are changed. **Do not start the Manager after `managersetup` is finished.**

> **Important:** When you run `managersetup`, you will see:
> *Do you want to run ESM in Compact or Distributed mode?*
> In this case, accept the default and keep moving through the wizard. You must follow this entire procedure to convert your ESM mode. Also, note that conversion from distributed correlation mode to compact mode is not supported.

8. Initialize certificate administration:

   ```
   bin/arcsight certadmin -init
   ```

   At this point, you are asked to create a password for the certificate administration and reenter it for the Password confirmation. Press **Enter**. For information on password restrictions, see the *ESM Administrator's Guide* section “Managing PasswordConfiguration”. Be sure to save this password in a safe place outside of ESM.
9. Add the version information for this node:

   ```
   /etc/init.d/arcsight_services setLocalBuildVersions
   ```
10. If a distributed cache instance is needed on the persistor node, set it up now:

    ```
    bin/arcsight dcachesetup
    ```

    See "Configuring a Distributed Cache" in the *ESM Administrator's Guide* for details on running `dcachesetup`.
11. Add correlators or aggregators as needed on the persistor node:

    ```
    bin/arcsight correlationsetup
    ```

    See "Configuring a Correlators and Aggregators" in the *ESM Administrator's Guide* for details on running `correlationsetup`.

The system is now in distributed mode.

To build the cluster (install ESM on the other nodes in the cluster):

In the *ESM Installation Guide*, see "Add Nodes to a Cluster - Further Node Installation" for details on adding cluster nodes. Select the distributed cache option to add a distributed cache instance and the correlation setup option to add aggregators and correlators.

To complete configuration and bring up the services:

> **Note:** Run these commands on the persistor, as the user *arcsight*, and from the directory `/opt/arcsight/manager`.

1. Set up passwordless SSH:

   ```
   /etc/init.d/arcsight_services sshSetup
   ```

2. Approve all certificates:

   ```
   bin/arcsight certadmin -approveall
   ```

3. Stop all services:

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

4. Start the repository service:

   ```
   /etc/init.d/arcsight_services start repo
   ```

5. Set up message bus control and message bus data:

   ```
   bin/arcsight mbussetup
   ```

   See "Configuring a Message Bus Control and Message Bus Data" in the *ESM Administrator's Guide* for details on running `mbussetup`.

6. If more repository instances are needed, add them now:

   ```
   bin/arcsight reposetup
   ```

7. Now start all services, which will bring up services related to distributed correlation mode:

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

8. Verify that all services are running:

   ```
   /etc/init.d/arcsight_services statusByNode
   ```

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 `/etc/localtime` is set correctly.

1. As user *arcsight*, shut down all arcsight services. (This is important.) Run `/etc/init.d/arcsight_services stop all`
2. As user `arcsight`, 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.

Import IPv6 Zone Package - Optional

If you are upgrading your system from ESM 6.11.0, and had updated that system with the Zone_Updates_<latest_version> zones, you can import IPv6 zones after a successful upgrade to 7.0 Patch 1. To do so, import the content package `ArcSight_IPV6_Zones.arb`, which is provided in the zip file

ArcSight_IPv6_Zones_<version>.zip. This ZIP file includes a readme file with installation instructions. The content package is available for download at https://marketplace.microfocus.com/arcsight. Select the category, **Utilities and Tools**.

Install Content Package - ArcSight SocView and ArcSight ClusterView (Optional)

The content packages are installed automatically when you perform a new ESM installation. However, when you upgrade your ESM system, the ArcSight SocView and ArcSight ClusterView content packages are not installed automatically. You can install these packages from the ArcSight Console any time after the upgrade.

On the Console, these packages are available from `//All Packages/ArcSight Foundation`.

- The SocView package provide dashboards for monitoring Analyst and case resolution activity in your security operations center (SOC). These dashboards are available on the ArcSight Command Center.
- The ClusterView package works for ESM with Distributed Correlation. When Distributed Correlation is operational, dashboards for monitoring clusters are available on the ArcSight Command Center.

For instructions on installing ESM packages, refer to the topic "Installing or Uninstalling Packages" in the *ArcSight Console User's Guide*.

Fix Invalid Resources

You checked for invalid resources before the upgrade and you will 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 a 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.

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 file at `<ARCSIGHT_HOME>/upgrade/out/<timestamp>/summary.html` to find invalid resources and fix their conditions as appropriate.

When the upgrade 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.

Caution: If you choose not to persist conflicts to the database and disable invalid resources, the ArcSight Manager might throw exceptions when the invalid resources try to evaluate live events.

1. Stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. As user *arcsight*, run:

   ```
   ./arcsight resvalidate -persist false
   ```

3. Start the Manager:

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

Install Netflow SmartConnectors

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

- 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 sales representative.

Delete Unassigned File Resources

The upgrade might result in unassigned resources. For example, the .art files are created as new file resources in ESM, 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

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 7.0 Patch 1 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 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.

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

It is also recommended that you verify whether the new 7.0 Patch 1 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**

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`.

Update Cases User Interface

Make sure you perform this post-upgrade task before upgrading ArcSight Console.

The upgrade includes the following changes to the Cases user interface:

- There are two new fields on the Cases UI:
  - Reason for Closure
  - Category of Situation
- The upgrade provides the file:

  `/opt/arcsight/manager/config/caseui.xml.orig`.

This topic covers two scenarios:

- If you *did not customize* the Cases user interface, at a minimum you are instructed to rename an XML file provided by the upgrade. This ensures that you will get any updates pertaining to user interface structure, for example, the new fields.
- If you customized the Cases user interface in a previous ESM version, you are instructed to restore any customized files manually. This is so that you will continue using those customizations and also access new Cases editor fields.

If you did not customize the Cases user interface:

1. Go to

   `/opt/arcsight/manager/config/`
2. Rename `caseui.xml` to something else, for example, `caseui.xml.old`. This is actually the pre-upgrade file which was not replaced by the upgrade.
3. Locate `caseui.xml.orig` which came with the upgrade, and rename it to `caseui.xml`.
4. Stop the Manager:

   `/etc/init.d/arcsight_services stop manager`

5. Start the services to implement the upgraded Cases structure and expose any new fields.

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

The updates will be propagated to both ArcSight Command Center and ArcSight Console.

If you customized the Cases user interface:

If you customized the Cases user interface 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. Locate the properties files you have previously customized (for example, `label_strings_en.properties` and `resource_strings_en.properties`, and other localized properties files) under `/opt/arcsight/manager.preUpgradeBackup/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.

   The upgrade process installs the latest properties files in `/opt/arcsight/manager/i18n/common`.
2. Open one customized properties file, for example, `/opt/arcsight/manager.preUpgradeBackup/i18n/common/label_strings_<locale>.properties`). Locate your customizations.

   Tip: Search for the string **extendedcase** to locate your customized field labels.
3. Copy the customizations in the corresponding properties file provided by the upgrade found in `/opt/arcsight/manager/i18n/common/`.

   Note: After upgrading ArcSight Console ("Upgrading ArcSight Console" on page 46), copy the following customized files to the individual Console installations at `arcsight\console\i18n\common\`:

   - `label_strings`
   - `resource_strings`
4. Rename the old `caseui.xml` file in `/opt/arcsight/manager/config/` to something like `caseui.xml.old`. This is the pre-upgraded file which was not replaced by the upgrade.
5. If you changed the UI structure, open your customized copy of `caseui.xml` under `/opt/arcsight/manager.preUpgradeBackup/config` . Locate the areas you changed.
6. Copy all of your structure changes to `caseui.xml.orig` found in `/opt/arcsight/manager/config/`

7. Rename `caseui.xml.orig` to `caseui.xml` (delete the .orig suffix).
8. 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`.
9. Stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```
10. Start services for these changes to take effect:

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

Re-apply and Verify Configurations

Restore and verify content after the upgrade.

1. If you created an `.arb` package in the topic "Prepare Resources for Upgrade" on page 6, import it and verify that its contents work as expected.
2. Verify that all resources work as expected.

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.

Configure ArcSight Investigate Access

You can configure access to ArcSight Investigate only after the upgrade. This configuration is optional.

To configure ESM access to ArcSight Investigate:

1. Log in as user *arcsight*, and stop the Manager services:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   ```
   ./arcsight managersetup -i console
   ```

3. Advance through the wizard until you get to the ArcSight Investigate panel.
4. Select whether to set up ArcSight Investigate. Select **Yes** to enable the integration; select **No** to continue. If you select **Yes**, specify the **Search URL** for the ArcSight Investigate deployment.
5. Continue to advance through the wizard and complete the configuration. For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide* .
6. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

Remove Deprecated Threat Response Manager (TRM) Integration Command Folders

The TRM integration commands are deprecated, and should no longer be used. To remove the TRM commands from the Integration Commands menu, delete the TRM folders. These folders are:

- /All Integration Commands/Deprecated/ArcSight Administration/TRM
- /All Integration Targets/Deprecated/ArcSight Administration/TRM
- /All Integration Configurations/Deprecated/ArcSight Administration/TRM

Re-register IPv6 Connectors

After the upgrade, you must re-register any connectors that support IPv6 addresses to facilitate correct data collection.

Configuring Event Broker Access - Event Broker 2.20

This section applies to Event Broker 2.20 only; if you have implemented Event Broker 2.21, see the section pertaining to that version.

In addition to the information in this section, refer to the *ESM Installation Guide* for details on Event Broker configuration and Event Broker Best Practices.

Configure Event Broker Access - Non-FIPS Mode (Optional) - Event Broker 2.20

You can configure access to the Event Broker only after the upgrade. This configuration is optional.

To configure ESM access to the Event Broker:

1. Log in as user *arcsight*, and stop the Manager:

   `/etc/init.d/arcsight_services stop manager`
2. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   `./arcsight managersetup -i console`
3. Advance through the wizard until you get to the Event Broker panel.
4. Select whether to set up connection to the Event Broker (if Event Broker is part of your implementation of ESM). Select **Yes** to set up the connection; select **No** to continue. If you select **Yes**, specify:
   a. **Host: Port(s)**: Enter the host (hostname or IP address) and port information for the nodes in the Event Broker. Include the host and port information of all the nodes in a multiple node environment not just the Master node. This is a comma-separated list, for example: <host>:<port>,<host>:<port>. Note that Event Broker can only accept IPV4 connections from ESM.

   b. **Topic to read from**: Specify the topic in the Event Broker you want to read from. This will determine the data source. See the chapter "Managing Event Broker Topics", in the *Event Broker Administrator's Guide*.

   c. **Path to the Event Broker root cert**: ESM communicates with the Event Broker through TLS. To enable this, you must import the Event Broker's root certificate into ESM's client truststore. Copy over the Event Broker root certificate from the Event Broker machine in this location: `/opt/arcsight/kubernetes/ssl/ca.crt` to a local folder on the ESM machine. After you enter the path to the certificate, and click **Next**, the Event Broker's root certificate is imported into ESM's client truststore and the connection to the Event Broker is validated. If there are any issues, you will receive an error or warning message. If no message displays and you advance to the next screen in the wizard, that indicates that the connection between the Event Broker and ESM is successfully validated.
5. Continue to advance through the wizard and complete the configuration. For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide* .
6. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

7. To verify that the connection to the Event Broker is working, look for `Event Broker service is initialized` in the `server.std.log`.

Setting Up SSL Client-Side Authentication Between Event Broker and ESM - Non-FIPS Mode (Optional) - Event Broker 2.20

Before setting up client-side authentication with Event Broker, you must import the Event Broker root certificate into the ESM truststore to enable the SSL handshake between the Event Broker and ESM.

To import the Event Broker root certificate into an ESM machine:

Note: Before performing the steps below to import the root certificate into the ESM truststore, check if the Event Broker root certificate has previously been imported into ESM. If it is not, then perform these steps:

1. Log onto the Event Broker machine and copy the certificate from the following location:

   `/opt/arcsight/kubernetes/ssl/ca.crt`

   into a location on the ESM machine.
2. Use the arcsight `keytool` command to import the root CA certificate into the ESM's client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```

To enable client-side authentication between the Event Broker and ESM for non-FIPS (default) mode:

IMPORTANT: All the steps in this procedure must be completed for client-side authorization to work. Be sure to perform all steps.

1. Verify that Event Broker is functional, and has client authentication set up.
2. As user *arcsight*, stop the Manager:

   `/etc/init.d/arcsight_services stop manager`
3. If `/opt/arcsight/manager/config/client.properties` does not exist, create it using an editor of your choice.
4. Change the store password for the keystore, `keystore.client`, which has an empty password by default. This empty password interferes with the certificate import you must perform.

   Also, you must update the empty password of the generated key `services-cn` in the keystore to be the same password as that of the keystore itself. To do so, run the following commands:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -storepasswd
-storepass ""
```

Enter the new password when prompted.

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -keypasswd -
keypass "" -alias services-cn
```

Enter the new password to be same as the store password (entered above), when prompted.

5. Update the password in `config/client.properties` by running this command:

   ```
   /opt/arcsight/manager/bin/arcsight changepassword -f
   config/client.properties -p ssl.keystore.password
   ```

6. Generate the keypair and certificate signing request (.csr) file. When generating the keypair, enter the fully qualified domain name of the manager host as the common name (CN) for the certificate. Run these commands:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair –
   dname "cn=<your host's fully qualified domain name>, ou=<your
   organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize
   2048 –alias ebkey -startdate -1d -validity 366
   ```

   ```
   /opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
   alias ebkey -file ebkey.csr
   ```

   where `ebkey.csr` is the output file where the `csr` is stored.

7. Sign the .csr with the Event Broker root certifcate. The Event Broker root certificate is on the Event Broker machine under `/opt/arcsight/kubernetes/ssl` and is called `ca.crt` and the key is called `ca.key`. For example, the following command can be run either on the Event Broker machine or on a different machine with a functional `openssl` as long as you have the `ca.crt` and `ca.key`:

   ```
   openssl x509 -req -CAkey <full path to ca.key> -CA <full path to ca.crt> -
   in <full path to the esm csr> -out <full path and file name for storing
   the generated cert> -days 3650 -CAcreateserial -sha256
   ```

   For example:

   ```
   openssl x509 -req -CAkey /tmp/ca.key -CA /tmp/ca.crt -in /tmp/ebkey.csr -
   out /tmp/ebkey.crt -days 3650 -CAcreateserial -sha256
   ```

   Note that all file locations must be specified with the full path.

8. On the ESM machine, import the signed certificate (the `-out` parameter in the above `openssl` command) by running this command:

   ```
   bin/arcsight keytool -store clientkeys -alias ebkey -importcert -file
   <path to signed cert> -trustcacerts
   ```

   For example:

   ```
   bin/arcsight keytool -store clientkeys -alias ebkey -importcert -file
   /tmp/ebkey.crt -trustcacerts
   ```

9. To verify that the configuration is complete, and the connection to Event Broker can be made successfully, run `managersetup` to verify that the configuration flows through with no errors.

10. Start the Manager:

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

Configure Event Broker Access - FIPS Mode (Server Authentication Only) (Optional) - Event Broker 2.20

You can configure access to the Event Broker only after the upgrade complete . This configuration is required only if ESM and Event Broker are in FIPS mode. The only FIPS mode supported for integration of ESM and Event Broker is FIPS 140-2.

To configure ESM access to the Event Broker in FIPS Mode:

1. Log in as user *arcsight*, and stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```
2. Log onto the Event Broker machine and copy the certificate from the following location:

   ```
   /opt/arcsight/kubernetes/ssl/ca.crt
   ```

   into a location on the ESM machine.
3. Use the arcsight `keytool` command to import the root CA certificate into the ESM's client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```
4. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   ```
   ./arcsight managersetup -i console
   ```

   For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide*.
5. Continue through the wizard until you encounter the Event Broker setup. Select **Yes** to set up the connection, and specify:
   a. **Host: Port(s)**: Enter the host (hostname or IP address) and port information for the nodes in the Event Broker. Include the host and port information of all the nodes in a multiple node environment not just the Master node. This is a comma-separated list, for example: <host>:<port>,<host>:<port>. Note that Event Broker can only accept IPV4 connections from ESM.

   b. **Topic to read from**: Specify the topic in the Event Broker you want to read from. This will determine the data source. See the chapter "Managing Event Broker Topics", in the *Event Broker Administrator's Guide*.

   c. **Path to the Event Broker root cert**: Do not enter a value in this field. You have already imported the certificate in step 3.

6. Click **Next**. The connection to the Event Broker is validated. If there are any issues, you will receive an error or warning message. If no message displays and you advance to the next screen in the wizard, that indicates that the connection between the Event Broker and ESM is successfully validated.
7. Continue to advance through the wizard and complete the configuration.
8. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

9. To verify that the connection to the Event Broker is working, look for `Event Broker service is initialized` in the `server.std.log`.

Setting Up SSL Client-Side Authentication Between Event Broker and ESM - FIPS Mode Event Broker 2.20

Before setting up client-side authentication with Event Broker, you must import the Event Broker root certificate into the ESM truststore to enable the SSL handshake between the Event Broker and ESM.

The only FIPS mode supported for integration of ESM and Event Broker is FIPS 140-2.

To import the Event Broker root certificate into an ESM machine:

Note: Before performing the steps below to import the root certificate into the ESM truststore, verify that the Event Broker root certificate has previously been imported into ESM. If it is not, then perform these steps:

1. Log onto the Event Broker machine and copy the certificate from the following location:

   `/opt/arcsight/kubernetes/ssl/ca.crt`

   into a location on the ESM machine.
2. Use the arcsight `keytool` command to import the root CA certificate into the ESM's client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```

To enable client-side authentication between the Event Broker and ESM for FIPS mode:

IMPORTANT: All the steps in this procedure must be completed for client-side authorization to work. Be sure to perform all steps.

1. Verify that Event Broker is functional, and has client authentication set up.
2. As user *arcsight*, stop the Manager:

```
/etc/init.d/arcsight_services stop manager
```

3. If `/opt/arcsight/manager/config/client.properties` does not exist, create it using an editor of your choice.
4. Generate the keypair and certificate signing request (.csr) file. When generating the keypair, enter the fully qualified domain name of the manager host as the common name (CN) for the certificate. Run these commands:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair –dname "cn=<your host's fully qualified domain name>, ou=<your organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize 2048 –alias ebkey -startdate -1d -validity 366
   ```

   ```
   /opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -alias ebkey -file ebkey.csr
   ```

   where `ebkey.csr` is the output file where the `csr` is stored.
5. Sign the .csr with the Event Broker root certifcate. The Event Broker root certificate is on the Event Broker machine under `/opt/arcsight/kubernetes/ssl` and is called `ca.crt` and the key is called `ca.key`. For example, the following command can be run either on the Event Broker machine or on a different machine with a functional `openssl` as long as you have the `ca.crt` and `ca.key`:

   ```
   openssl x509 -req -CAkey <full path to ca.key> -CA <full path to ca.crt> -in <full path to the esm csr> -out <full path and file name for storing the generated cert> -days 3650 -CAcreateserial -sha256
   ```

   For example:

   ```
   openssl x509 -req -CAkey /tmp/ca.key -CA /tmp/ca.crt -in /tmp/ebkey.csr -out /tmp/ebkey.crt -days 3650 -CAcreateserial -sha256
   ```

   Note that all file locations must be specified with the full path.
6. On the ESM machine, import the signed certificate (the `-out` parameter in the above `openssl` command) by running this command:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey -importcert -file <path to signed cert> -trustcacerts
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey -importcert -file /tmp/ebkey.crt -trustcacerts
   ```
7. To verify that the configuration is complete, and the connection to Event Broker can be made successfully, run `managersetup` to verify that the configuration flows through with no errors.
8. Start the Manager:

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

Configuring Event Broker Access - Event Broker 2.21

This section applies to Event Broker 2.21 only; if you have implemented Event Broker 2.20, see the section pertaining to that version.

In addition to the information in this section, refer to the *ESM Installation Guide* for details on Event Broker configuration and Event Broker Best Practices.

Configure Event Broker Access - Non-FIPS Mode (Optional) - Event Broker 2.21

You can configure access to the Event Broker only after the upgrade. This configuration is optional.

To configure ESM access to the Event Broker:

1. Log in as user *arcsight*, and stop the Manager:

   `/etc/init.d/arcsight_services stop manager`
2. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   `./arcsight managersetup -i console`
3. Advance through the wizard until you get to the Event Broker panel.
4. Select whether to set up connection to the Event Broker (if Event Broker is part of your implementation of ESM). Select **Yes** to set up the connection; select **No** to continue. If you select **Yes**, specify:
   a. **Host: Port(s)**: Enter the host (hostname or IP address) and port information for the nodes in the Event Broker. Include the host and port information of all the nodes in a multiple node environment not just the Master node. This is a comma-separated list, for example: <host>:<port>,<host>:<port>. Note that Event Broker can only accept IPV4 connections from ESM.

   b. **Topic to read from**: Specify the topic in the Event Broker you want to read from. This will determine the data source. See the chapter "Managing Event Broker Topics", in the *Event Broker Administrator's Guide*.

   c. **Path to the Event Broker root cert**: ESM communicates with the Event Broker through TLS. To enable this, you must import the Event Broker's root certificate into ESM's client truststore. Copy over the Event Broker root certificate from the Event Broker machine in this location: `/opt/arcsight/kubernetes/scripts/arcsight-cert-util.sh > /tmp/ca.crt` to a local folder on the ESM machine. After you enter the path to the certificate, and click **Next**, the Event Broker's root certificate is imported into ESM's client truststore and the connection to the Event Broker is validated. If there are any issues, you will receive an error or warning

message. If no message displays and you advance to the next screen in the wizard, that indicates that the connection between the Event Broker and ESM is successfully validated.

5. Continue to advance through the wizard and complete the configuration. For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide* .
6. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

7. To verify that the connection to the Event Broker is working, look for `Event Broker service is initialized` in the `server.std.log`.

Setting Up SSL Client-Side Authentication Between Event Broker and ESM - Non-FIPS Mode (Optional) - Event Broker 2.21

Before setting up client-side authentication with Event Broker, you must import the Event Broker root certificate into the ESM truststore to enable the SSL handshake between the Event Broker and ESM.

To import the Event Broker root certificate into an ESM machine:

Note: Before performing the steps below to import the root certificate into the ESM truststore, check if the Event Broker root certificate has previously been imported into ESM. If it is not, then perform these steps:

1. Log onto the Event Broker machine and copy the certificate from the following location:

   `/opt/arcsight/kubernetes/scripts/arcsight-cert-util.sh > /tmp/ca.cert.pem`

   into a location on the ESM machine.
2. Use the arcsight `keytool` command to import the root CA certificate into the ESM's client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert -file <absolute path to certificate file> -alias <alias for the certificate>
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias alias1 -importcert -file /tmp/ca.cert.pem
   ```

To enable client-side authentication between the Event Broker and ESM for non-FIPS (default) mode:

IMPORTANT: All the steps in this procedure must be completed for client-side authorization to work. Be sure to perform all steps.

1. When Event Broker is first installed, it is set up to use self-signed certificates. To replace the self-signed certificates, obtain your company's root CA certificate, an intermediate certificate, and key pair. Place them in `/tmp` with the following names:
   - `/tmp/intermediate.cert.pem`
   - `/tmp/intermediate.key.pem`
   - `/tmp/ca.cert.pem`
2. Verify that Event Broker is functional, and has client authentication set up.
3. As user *arcsight*, stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```
4. If `/opt/arcsight/manager/config/client.properties` does not exist, create it using an editor of your choice.
5. Change the store password for the keystore, `keystore.client`, which has an empty password by default. This empty password interferes with the certificate import you must perform.

   Also, you must update the empty password of the generated key `services-cn` in the keystore to be the same password as that of the keystore itself. To do so, run the following commands:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -storepasswd
   -storepass ""
   ```

   Enter the new password when prompted.

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -keypasswd -
   keypass "" -alias services-cn
   ```

   Enter the new password to be same as the store password (entered above), when prompted.
6. Update the password in `config/client.properties` by running this command:

   ```
   /opt/arcsight/manager/bin/arcsight changepassword -f
   config/client.properties -p ssl.keystore.password
   ```
7. Generate the keypair and certificate signing request (.csr) file. When generating the keypair, enter the fully qualified domain name of the manager host as the common name (CN) for the certificate. Run these commands:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair –
   dname "cn=<your host's fully qualified domain name>, ou=<your
   organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize
   2048 –alias ebkey -startdate -1d -validity 366
   ```

```
/opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
alias ebkey -file ebkey.csr
```

where `ebkey.csr` is the output file where the `csr` is stored.

8. Sign the .csr with the Event Broker root certifcate. The Event Broker root certificate is on the Event Broker machine under `/opt/arcsight/kubernetes/ssl` and is called `intermediate.cert.pem` and the key is called `ca.key`. For example, the following command can be run either on the Event Broker machine or on a different machine with a functional `openssl` as long as you have the `intermediate.cert.pem` and `intermediate.key.pem`:

   ```
   openssl x509 -req -CA ${INTERMEDIATE_CA_CRT} -CAkey ${INTERMEDIATE_CA_KEY}
   -in <full path to the esm csr> -out <full path and file name for
   storingthe generated cert> -days 3650 -CAcreateserial -sha256
   ```

   For example:

   ```
   openssl x509 -req -CA /tmp/intermediate.cert.pem -CAkey
   /tmp/intermediate.key.pem -in /tmp/ebkey.csr -out
   /tmp/signedIntermediateEBkey.crt -days 3650 -CAcreateserial -sha256
   ```

   Note that all file locations must be specified with the full path.

9. Import the intermediate cert from Event Broker into the ESM client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
   <alias for the certificate> -importcert -file <absolute path to
   certificate file>
   ```

   For example:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -alias
   ebcaroot -importcert -file /tmp/intermediate.cert.pem
   ```

10. On the ESM machine, import the signed certificate (the `-out` parameter in the above `openssl` command) by running this command:

    ```
    /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
    -importcert -file <path to signed cert> -trustcacerts
    ```

    For example:

    ```
    /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias ebkey
    -importcert -file /tmp/signedIntermediateEBkey.crt -trustcacerts
    ```

11. To verify that the configuration is complete, and the connection to Event Broker can be made successfully, run `managersetup` to verify that the configuration flows through with no errors.
12. Start the Manager:

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

Configure Event Broker Access - FIPS Mode (Server Authentication Only) (Optional) - Event Broker 2.21

You can configure access to the Event Broker only after the upgrade complete . This configuration is required only if ESM and Event Broker are in FIPS mode. The only FIPS mode supported for integration of ESM and Event Broker is FIPS 140-2.

To configure ESM access to the Event Broker in FIPS Mode:

1. Log in as user *arcsight*, and stop the Manager:

   `/etc/init.d/arcsight_services stop manager`
2. Log onto the Event Broker machine and copy the certificate from the following location:

   `/opt/arcsight/kubernetes/scripts/arcsight-cert-util.sh > /tmp/ca.crt`

   into a location on the ESM machine.
3. Use the arcsight `keytool` command to import the root CA certificate into the ESM's client truststore:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert
   -file <absolute path to certificate file> -alias <alias for the
   certificate>
   ```
4. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   `./arcsight managersetup -i console`

   For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide*.
5. Continue through the wizard until you encounter the Event Broker setup. Select **Yes** to set up the connection, and specify:
   a. **Host: Port(s)**: Enter the host (hostname or IP address) and port information for the nodes in the Event Broker. Include the host and port information of all the nodes in a multiple node environment not just the Master node. This is a comma-separated list, for example: <host>:<port>,<host>:<port>. Note that Event Broker can only accept IPV4 connections from ESM.
   b. **Topic to read from**: Specify the topic in the Event Broker you want to read from. This will determine the data source. See the chapter "Managing Event Broker Topics", in the *Event Broker Administrator's Guide*.
   c. **Path to the Event Broker root cert**: Do not enter a value in this field. You have already imported the certificate in step 3.
6. Click **Next**. The connection to the Event Broker is validated. If there are any issues, you will receive an error or warning message. If no message displays and you advance to the next screen in the

wizard, that indicates that the connection between the Event Broker and ESM is successfully validated.

7. Continue to advance through the wizard and complete the configuration.
8. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

9. To verify that the connection to the Event Broker is working, look for `Event Broker service is initialized` in the `server.std.log`.

Configure Integration with ServiceNow® IT Service Management (ITSM) - Optional

You can optionally configure to integrate with the ServiceNow® IT Service Management (ITSM) application after upgrade.

To configure ESM integrate with ServiceNow® IT Service Management (ITSM):

1. Log in as user *arcsight*, and stop the Manager services:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. As user *arcsight* , start the `managersetup` wizard by running the following command from the `/opt/arcsight/manager/bin` directory:

   ```
   ./arcsight managersetup -i console
   ```

3. Advance through the wizard until you get to the ServiceNow® IT Service Management (ITSM) panel.
4. Select whether to set up ServiceNow® IT Service Management (ITSM). Select **Yes** to enable the integration; select **No** to continue. If you select **Yes**, specify the **ServiceNow URL** and the optional **ServiceNow Proxy URL**.
5. Continue to advance through the wizard and complete the configuration. For details about running the Manager Configuration Wizard (`managersetup`), see "Using the Configuration Wizard" in the *ESM Administrator's Guide* .
6. When you have completed the configuration, restart the Manager by running the following as user *arcsight*:

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

Check Existing Content After Upgrade

After the upgrade is completed, verify that all your content has been successfully transferred to the 7.0 Patch 1 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: It is recommended not to move these resources into any ArcSight standard content groups, because they will move to the Unassigned group during future upgrades.

  However, the .art files are created as new file resources in ESM, 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 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 7.0 Patch 1. This may happen for assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In 7.0 Patch 1, 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
  ```

- **Check user's ACLs**. After the upgrade, verify that your user ACLs are correct and still valid based on how ArcSight standard content is organized for 7.0 Patch 1. 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.
- **Check zones resources**. 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 7.0 Patch 1 zone. Do not import the old zone.
- **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 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 7.0 Patch 1, 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.
- As of ESM 7.0 Patch 1, the data monitors Session Reconciliation and Event Reconciliation are deprecated are removed from the ArcSight Console. They are listed in the ArcSight Console after ESM upgrade, but these data monitors are no longer available.

Disable Intrusion Monitor Resources

As of ESM 7.0 Patch 1, you must disable Intrusion Monitoring resources. Intrusion Monitoring was installed part of System Content in ESM prior to ESM 6.8.

To disable Intrusion Monitor resources:

1. In the ArcSight Console's resource navigator, locate these resources:
   - Data monitors under `/All Data Monitors/ArcSight Foundation/Intrusion Monitoring/`
   - Rules under `/All Rules/ArcSight Foundation/Intrusion Monitoring/`
   - Trends under `/All Trends/ArcSight Foundation/Intrusion Monitoring/`
2. Right-click each resource and choose **Disable**.

Chapter 4: 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 the download web site. The xxxx in the file name represents the Console build number:
   - `ArcSight-7.0.0.xxxx.1-Console-Win.exe`
   - `ArcSight-7.0.0.xxxx.1-Console-Linux.bin`
   - `ArcSight-7.0.0.xxxx.1-Console-MacOSX.zip`
3. If you downloaded the ESM 7.0 Patch 1 Console installation file to a different machine, transfer it to the machine on which you plan to install the Console.

Run the ESM 7.0 Patch 1 Console Installation

1. Run the installation file appropriate for your platform:
   - **On Windows**:
     Double-click `ArcSight-7.0.0.xxxx.1-Console-Win.exe`
   - **On Macintosh:**
     Unzip the following file:

     ```
     ArcSight-7.0.0.xxxx.1-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-7.0.0.xxxx.1-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-7.0.0.xxxx.1-Console-Linux.bin -i console
     ```

Step through the Installation wizard screens to use the graphical user interface mode for installation. 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 license terms checkbox will be disabled until you read and scroll to the bottom of the agreement text. After you have read the text, select the checkbox associated with **I accept the terms of the License Agreement**. Click **Next**.
- **Special Notice:** Read the notice and click **Next**.
- **Choose Installation Folder:** Enter an `<ARCSIGHT_HOME>` path for 7.0 Patch 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**.
4. On this screen, previous configuration settings are displayed with a dropdown the options **IPv4** and **IPv6**. Select one of the IP types, depending on your ESM server configuration. Click **Next** to continue and complete the configuration and installation.

Run the ESM 7.0 Patch 1 Console Configuration

See the *ESM Installation 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."

Before starting the ArcSight Console:

If you customized your Cases UI in the previous version, it is assumed you followed the post-Manager upgrade task described in "Update Cases User Interface" on page 27. At step 3, you were reminded to copy these two files over to the Console's `arcsight\console\i18n\common\ directory:`

- `label_strings`
- `resource_strings`

After copying the above files over to the Console directory, start the ArcSight Console.

Post-Console Upgrade Tasks

Note: Event Reconciliation and Session Reconciliation data monitors

Beginning with ESM 7.0 Patch 1, the Event Reconciliation and Session Reconciliation data monitors are deprecated. If you created any of these data monitors for your own use, these are not functional after the upgrade. On the Console resource navigator, the resources will appear as invalid (broken icon).

1. If you previously customized any field labels on the Cases UI, see "Update Cases User Interface" on page 27 for instructions on what to do with the label properties files.
2. After you have upgraded a Console to 7.0 Patch 1 check to verify that:
   a. You can view the upgraded standard content.
   b. Your customized Cases UI labels are displaying correctly.
   c. All your SmartConnectors are connecting to the Manager.
   d. 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 5: Upgrading ArcSight SmartConnectors

Note: It is recommended 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.

ArcSight Forwarding Connectors must be upgraded only after their corresponding source/destination ESMs have been upgraded. The Forwarding Connectors must be the version that shipped with ESM, or the latest version. See the ESM Support Matrix to verify the version of Forwarding Connector to install.

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

This chapter describes the method for upgrading a multi-ESM deployment to 7.0 Patch 1.

Multi-ESM Deployments

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 source/destination 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 top tier ESM.

1. Upgrade any SmartConnectors that are not running a recent version. For best results, use the latest available SmartConnector version.
2. Remove the ArcSight services on the current ESM.
3. Follow instructions in "Running the Upgrade" on page 14 to upgrade your ESM to 7.0 Patch 1.
4. Once ESM 7.0 Patch 1 is running, follow instructions in the "Upgrading ArcSight Console" on page 46 to upgrade any Consoles connected to it.
5. To upgrade the Forwarding Connector, the source/destination ESMs must be upgraded first. For details, see the ArcSight Forwarding Connector Configuration Guide, and the ESM Support Matrix.

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

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

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Upgrade Guide (ESM 7.0 Patch 1)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!