Micro Focus Security ArcSight ESM

Software Version: 7.6.4

Upgrade Guide

Legal Notices

Copyright Notice

Trademark Notices

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://www.microfocus.com/documentation/arcsight/

Contents

Chapter 1: Preparing to Upgrade 5
Understanding Supported Upgrade Paths 5
Understanding Supported Operating Systems on an Appliance 6
Completing Pre-Upgrade Tasks 7
Running the Resource Validator 10
Preparing Resources for Upgrade 11
Backing Up Resources Before Upgrading 12
Ensuring Correct File Permissions 13
Software ESM: Installing the Time Zone Package 13
Testing the Upgrade 14
Chapter 2: Running the Upgrade 17
Upgrading Software ESM 17
Upgrading Software ESM in Compact Mode 18
Upgrading Software ESM in Distributed Correlation Mode 21
Upgrading ESM on an Appliance 24
Upgrading the Operating System on a B7600 (G9) or B7700 (G10) Appliance 25
Upgrading the Appliance to ESM 7.6.4 26
Upgrading a Hierarchical or Other Multi-ESM Installation 28
Verifying Successful Upgrade 29
Reporting Upgrade Issues 30
Chapter 3: Completing Post-Upgrade Tasks 32
Completing Required Post-Upgrade Tasks 32
Restoring or Deleting Deprecated Resources 34
Updating the Cases User Interface 35
Restoring and Verifying Customized Standard Resources 36
Verifying Content Transfer 37
Completing Optional Post-Upgrade Tasks 38
Converting from Compact Mode to Distributed Correlation Mode 41
Appliance: Converting to Prefer IPv6 43
Configuring Recon Access 44
Configuring Transformation Hub Access - Non-FIPS Mode 45
Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode 46
Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only) 49
Configuring Integration with ServiceNow® IT Service Management (ITSM) 51
Chapter 4: Upgrading the ArcSight Console and Smart Connectors 52
Upgrading the ArcSight Console 52

Upgrading ArcSight SmartConnectors 53
Publication Status 54

Send Documentation Feedback 55

Chapter 1: Preparing to Upgrade

This document describes the steps required to upgrade software ESM or ESM on an appliance to version 7.6. This chapter describes how to prepare your environment for upgrade.

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

You install software ESM on your own hardware.

For information about upgrading in a high availability environment, see the Active Passive High Availability Module User's Guide.

Note: Ensure you perform the upgrade from a local workstation or server, not over a VPN. If you perform the upgrade over a VPN, and the VPN is disconnected during the upgrade, the upgrade will fail. If you must use a VPN during the upgrade process, consider using a desktop sharing utility like the `screen` command on Linux to prevent terminating the upgrade session if the network disconnects.

Understanding Supported Upgrade Paths

The following upgrade paths are supported for software ESM (in both compact mode and distributed correlation mode) and ESM on an appliance:

- For ESM 6.11, with or without patches:
  a. Upgrade to ESM 7.0 Patch 1.
  b. Upgrade to ESM 7.2.
  c. Upgrade to ESM 7.4.
  d. Upgrade to ESM 7.5.
  e. Upgrade to ESM 7.6.
- For ESM 7.0:
  a. Apply ESM 7.0 Patch 2.
  b. Upgrade to ESM 7.2.
  c. Upgrade to ESM 7.4.
  d. Upgrade to ESM 7.5.
  e. Upgrade to ESM 7.6.
- For ESM 7.0 Patch 1 and Patch 2:
  a. Upgrade to ESM 7.2.
  b. Upgrade to ESM 7.4.

c. Upgrade to ESM 7.5.
d. Upgrade to ESM 7.6.

- For ESM 7.2 and ESM 7.3:
  a. Upgrade to ESM 7.4.
  b. Upgrade to ESM 7.5.
  c. Upgrade to ESM 7.6.
- For ESM 7.2 Service Pack 1:
  a. Upgrade to ESM 7.3.
  b. Upgrade to ESM 7.5.
  c. Upgrade to ESM 7.6.
- For ESM 7.4:
  a. Upgrade to ESM 7.5.
  b. Upgrade to ESM 7.6.
- For ESM 7.5, you can upgrade directly to ESM 7.6.

For information about supported platforms, see the Technical Requirements.

Note: If you are running ESM in compact mode and want to convert to distributed correlation mode, complete the upgrade to ESM 7.6 as described in Running the Upgrade, and then convert the system to distributed correlation mode as described in Converting from Compact Mode to Distributed Correlation Mode. Conversion to distributed correlation mode is not supported on an appliance.

Understanding Supported Operating Systems on an Appliance

ESM 7.6 supports the following appliances and operating systems:

- B7700 (G10) appliances running on RHEL 7.9.

  If you are running ESM 7.2 on a G10 appliance that is running RHEL 7.7, you must:
  - Upgrade the operating system to RHEL 7.8 and ESM to version 7.4.
  - Upgrade the operating system to RHEL 7.9 and ESM to version 7.5.
  - Perform an operating system update to RHEL 7.9.
  - Upgrade to ESM version 7.6.

  If you are running ESM 7.2 on a G10 appliance that is running RHEL 7.7, you must upgrade the operating system to RHEL 7.9 before you upgrade to ESM 7.6.
- B7600 (G9) appliances running on RHEL 7.9.

If you are running ESM 6.11 on a G9 appliance that is running RHEL 7.3, after you upgrade the appliance to ESM 7.0 Patch 1 and RHEL 7.5, you must upgrade the operating system first to RHEL 7.5, then to RHEL 7.7, then to RHEL 7.8, and then to RHEL 7.9

For more information about upgrading an appliance, see Upgrading ESM on an Appliance

Completing Pre-Upgrade Tasks

This section describes tasks to complete in order to ensure a successful upgrade.

Note: 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 cannot change the file system type after installation, even during an upgrade.

To prepare your system for upgrade:

1. Because the upgrade program requires that the MySQL `root` user password and the MySQL `arcsight` user password are identical, log in as both users to verify that the passwords are identical:

   ```
   /opt/arcsight/logger/current/arcsight/bin/mysql -u arcsight -p
   ```

   ```
   /opt/arcsight/logger/current/arcsight/bin/mysql -u root -p
   ```

   If the passwords are not identical, contact Technical Support for information about changing them so that they are identical for the duration of the upgrade.

2. If you have connectors that are version 7.15 or earlier, add the `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` cipher suite to `<connector>\current\config\agent\agent.defaults.properties` and restart the connectors.

   In non-FIPS environments, the complete list of cipher suites should be as follows:

   ```
   ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ```

   In FIPS environments, the complete list of cipher suites should be as follows:

   ```
   ssl.fips.cipher.suites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ```

   ```
   ssl.fips.suiteb.128.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
   ```

   ```
   ssl.fips.suiteb.192.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
   ```

3. Verify that your current software ESM or ESM on an appliance is fully functional and that archives are intact.

   If there is an issue with your existing system, contact Technical Support before you start the upgrade.

4. Run the resource validator (`resvalidate`) and fix invalid resources.

   For more information, see Running the Resource Validator.

5. If you are a Premier/Flexcare customer seeking upgrade support by using your Flex credits, contact Technical Support to discuss upgrade assistance.

6. Copy the `/opt/arcsight` directory or complete tasks in the CORR-Engine Backup and Recovery Tech Note to create a backup copy of the system.

   Caution: To avoid issues, complete the upgrade immediately after you back up the system.

   If you do not want to back up events and archives, you can exclude the following directories from the backup:

   - `/opt/arcsight/logger/data/archives`
   - `/opt/arcsight/logger/data/indexes`
   - `/opt/arcsight/logger/data/logger`

   Note: After you restore the backup, ensure that the `/opt/arcsight/logger/data/logger/` directory exists before you start the services. Otherwise, the `loggerd` service will not start.

   The logger directories cannot be used to roll back a logger upgrade failure, but Technical Support might request them in order to investigate recovery options.

7. Prepare your resources for upgrade.

   For more information, see Preparing Resources for Upgrade.

8. Ensure that your ESM installation has the correct file permissions.

   For more information, see Ensuring Correct File Permissions

9. If you are upgrading software ESM, ensure that the `/opt` directory has at least 50 GB of free space and that the `/tmp` directory has at least 5 GB of free space.

   Caution: Do not mount `/opt` or `/opt/arcsight` to the `/tmp` directory. Linux has a cleanup process that deletes files under `/tmp`. Subsequently, you will risk losing your ESM installation.

10. Set the Java (Manager) heap size.

    Micro Focus recommends changing the Java heap size to at least 16 GB before you upgrade. If the heap size is less than 16 GB, the upgrade program displays a message

recommending that you increase the heap size to at least 16 GB after the upgrade is complete.

To avoid that message, as user `arcsight`, run `/opt/arcsight/manager/bin/arcsight managersetup` to increase the Java heap size. For more information about `managersetup`, see the ESM Administrator's Guide.

11. If you are upgrading software ESM, install the time zone package.

    For more information, see Software ESM: Installing the Time Zone Package.

12. Depending on your environment, install the following libraries:
    - If you are upgrading in a RedHat or CentOS 8.1 environment:
      - ncurses-compat-libs
      - libnsl
      - libaio
      - numactl
    - If you are upgrading in a SUSE Enterprise Linux 15 SP 1 environment:
      - libncurses5
      - libaio1
      - numactl
    - If you are upgrading in a SUSE Enterprise Linux 12 SP 4 environment:
      - libaio1
      - numactl
    - For all other environments:
      - libaio
      - numactl
13. If you are upgrading software ESM, install an entropy generator (normally provided by your operating system vendor) such `rng-tools` or `haveged`. ESM requires high levels of operating system entropy for secure cryptography.
14. If you are upgrading ESM in a RedHat or CentOS environment running X Windows, either download and install the required RPM package (`LibXtst.x86_64`) from https://centos.pkgs.org/7/centos-x86_64/libXtst-1.2.3-1.el7.x86_64.rpm.html or run the following command to install the `LibXtst.so.6` library:

    ```
    yum install libXtst
    ```

15. Download `ArcSightESMSuite-7.6.0.xxxx.0.tar` from the Licensing and Downloads site (where `xxxx` is the build number) and copy the file to the system you will be upgrading.

Micro Focus provides a digital public key to enable you to verify that the signed software that you received is from Micro Focus and has not been manipulated by a third party. For more information and instructions, visit the Signature Verification page.

To initiate license procurement, after you download the `.tar` file, follow the instructions in the Electronic Delivery Receipt that you receive in e-mail.

16. Test the upgrade before you upgrade your production environment.

    For more information, see Testing the Upgrade.

Running the Resource Validator

Run the resource validator (`resvalidate`) and fix all invalid resources before you start the upgrade process. After the upgrade process is complete, run the resource validator again to see if a change in the schema rendered any resources invalid. For more information about fixing invalid resources, see Completing Required Post-Upgrade Tasks.

The resource validator verifies that the values expressed in the resource condition statement still apply to the resource, and that any resources upon which it depends are present and 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

To run the resource validator:

1. Stop the ArcSight Manager:

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

2. As user `arcsight`, run the following command:

   ```
   /opt/arcsight/manager/bin/arcsight resvalidate -persist false
   ```

   The resource validator generates `validationReport.html` and `validationReport.xml` in the `/opt/arcsight/manager` directory. Save these files to another directory so that you can compare them to the files that are generated after the upgrade.

3. Restart the ArcSight Manager:

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

After the upgrade is complete, run `resvalidate` again.

Preparing Resources for Upgrade

This section describes how the upgrade affects your resources and how to prepare your resources for upgrade.

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

Standard, ESM-supplied resources are refreshed with new versions during upgrade. If you copied these resources to a custom group and then customized them, the upgrade does not affect the custom group.

If you customized standard resources in their original location, back up the resources to an `.arb` file (exclude related resources) before you upgrade. You can restore the resources after the upgrade is complete.

Note: When you restore an `.arb` file, you overwrite the version that the upgrade program provided. If the upgrade included improvements, the improvements will not be available. As an option, you can apply your customizations to the new version.

The upgrade does not affect the following customizations:

- Asset modeling for network assets, including the following:
  - 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

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

Backing Up Resources Before Upgrading

Back up standard resources that you customized in their original location (not resources that you moved to a custom group), including active lists.

Note: The upgrade program does not preserve active list attributes such as the Time to Live (TTL) and description. The upgrade program does preserve entries that were added to active lists.

To back up resources:

1. In the ArcSight Console, for each resource type (filter, rule, active list, etc.), create a new group under your personal group and provide a name that identifies the contents.
2. Copy the resources to the new group.

   Any resources that point to other resources remain unchanged; they still point to the other resource even if you also copied that resource. You must correct the pointers to point to the copied version.
3. Export the backup groups in a package:
   a. From 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. Right-click the group that you created and select **Add to Package**.
   c. Select your new package and click **OK**.
   d. Right-click your package name and select **Export Package to Bundle**.

Tip: Copy and paste configurations from the old resources to the new resources after the upgrade is complete.

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.

Ensuring Correct File Permissions

The upgrade program checks your system to prevent upgrade failures due to incorrect file permissions. To avoid upgrade failures, you can manually perform these checks before you start the upgrade. Ensure that your ESM installation has the following file permissions:

- User `arcsight` should own `/opt/arcsight/` and all files and directories below it.
- `/opt/arcsight` and all directories below it should have a minimum permission of 500. This is the minimum permission that allows the `arcsight` user to list files within a directory.
- All files within `/opt/arcsight` or any subdirectory should have a minimum permission of 400. This is the minimum permission for the `arcsight` user to read the contents of the files.

If your ESM installation does not meet these requirements, you will need to resolve the issues before you can proceed with the upgrade.

Note: There are some exceptions. User `root` is expected to own the files `/opt/arcsight/manager/bin/setup_ services.sh` , `/opt/arcsight/manager/bin/remove_ services.sh`, and the contents of the `/opt/arcsight/services/highavail` directory. The `arcsight` user does not need to own these files.

Software ESM: Installing the Time Zone Package

This section does not apply to ESM on an appliance.

ESM uses the time zone update package to automatically handle changes in time zone or changes between standard and daylight savings time. During the upgrade, ESM verifies whether the appropriate operating system time zone update package is installed. If it is not, you have the option to exit the upgrade program and install the latest package or continue the ESM upgrade and install the time zone update package later. Micro Focus recommends installing the time zone update package when prompted.

The package to use depends on your operating system version:

For this operating system:	Use this package or later:
RHEL or CentOS 8.4	`tzdata-2020f-1.el8.noarch.rpm`
RHEL or CentOS 8.2	`tzdata-2020f-1.el8.noarch.rpm`
RHEL or CentOS 8.1	`tzdata-2020f-1.el8.noarch.rpm`
RHEL or CentOS 7.8	`tzdata-2020f-1.el7.noarch.rpm`

RHEL or CentOS 7.7	`tzdata-2020f-1.el7.noarch.rpm`
SLES 15 Service Pack 1	`timezone-2020f-3.41.2.x86_64.rpm`
SLES 12 Service Pack 5	`timezone-2020f-74.46.1.x86_64.rpm`

To install the time zone update package before upgrade:

1. Unpack the package and upload it to your server (for example, to `/opt/work/<package name>`).
2. As user `root`, run the following command:

   ```
   rpm -Uvh /opt/work/<package name>
   ```

3. To check the time zone setting, run the following command:

   ```
   timedatectl
   ```

4. If the time zone is not correct or it is not the desired time zone, run the following command to specify another time zone:

   ```
   timedatectl set-timezone <time zone>
   ```

   For example:

   ```
   timedatectl set-timezone America/Los_Angeles
   ```

To install the time zone update package after the upgrade is complete:

1. Use the procedure above to install the correct time zone update package.
2. As user `arcsight`, shut down all ArcSight services:

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

3. As user `arcsight`, run the following command (all on one line):

   ```
   /opt/arcsight/manager/jre/bin/java -jar /opt/arcsight/manager/lib/jre-tools/tzupdater/ziupdater-1.0.1.2.jar -V
   ```

4. As user `arcsight`, start all ArcSight services:

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

Testing the Upgrade

Micro Focus recommends testing the upgrade before you upgrade your production environment. This section provides an example of how to perform this test.

To test the upgrade:

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

   Note: You must complete the remaining steps as user `arcsight`.
2. Stop the ArcSight 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. If the production environment is in compact mode, start the ArcSight Manager in the production environment:

   ```
   /etc/init.d/arcsight_services start manager
   ```
5. If the production environment is in distributed mode, stop all services and then restart them:

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

   ```
   /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 ArcSight 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. If the test environment is in compact mode, start the ArcSight Manager in the test environment:

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

10. If the test environment is in distributed mode, stop all services and then restart them:

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

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

11. Verify that the ArcSight Manager in the test environment is functioning.
12. Stop the ArcSight Manager in the test environment:

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

13. Verify that the ArcSight Manager for the test system is completely shut down and that the `mysql` service is available.
14. Run `resvalidate` to validate resources.

    For more information, see Running the Resource Validator.
15. Proceed with the upgrade procedure in the test environment.

    For more information, see Running the Upgrade.

Chapter 2: Running the Upgrade

This chapter describes the steps required to upgrade your system from software ESM or ESM on an appliance to ESM 7.6.

Before you start the upgrade, complete the tasks in Completing Pre-Upgrade Tasks.

For information about upgrading software ESM, see Upgrading Software ESM.

For information about upgrading on an appliance, see Upgrading ESM on an Appliance .

For information about upgrading a hierarchical or other multi-ESM deployment, see Upgrading a Hierarchical or Other Multi-ESM Installation.

Note: Ensure you run the installer from a directory that is both owned by the arcsight user and outside the current ESM home directory (typically `/opt/arcsight/`). For example, you can use either the `/home/arcsight/` or `/opt/installer/` directories.

Upgrading Software ESM

This section describes how to upgrade software ESM in compact mode and software ESM in distributed mode.

Notes:

- For software ESM, running the upgrade in GUI mode is optional. To run the upgrade in GUI mode, install the X Windows system package for your operating system. Micro Focus recommends running the upgrade in console mode rather than GUI mode.
- X Windows is not included in the operating system image provided on a G9 appliance. If you are upgrading ESM on an appliance, use console mode.
- In GUI mode, if the upgrade program displays a dialog reporting an error or problem, click **Quit** to close the dialog. Micro Focus does not recommend using the **X** to close the dialog.

In both GUI mode and console mode, the upgrade process displays ongoing status updates with details about what it is doing. For example, `Upgrading database`, `Updating startup scripts`, or `Completing installation`.

ESM also generates status messages in `/opt/arcsight/upgradelogs/suite_upgrade.log` so that you can view the upgrade progress. If you are upgrading ESM in compact mode or on the persistor node in distributed correlation mode, typical log messages are as follows:

```
[2020-06-25 18:57:48.198 PDT] PROGRESS: "Storage Engine Upgrade" started. To go - Phase: 7.6 Total: 15.7 minutes estimate.
```

```
[2020-06-25 19:02:40.707 PDT] PROGRESS: "Storage Engine Upgrade" completed. 48% complete, about 7.6 minutes to go.
```

```
[2020-06-25 19:02:40.938 PDT] PROGRESS: "Start Storage Engine" started. To go
- Phase: 2.3 Total: 6.9 minutes estimate.

[2020-06-25 19:05:28.819 PDT] PROGRESS: "Start Storage Engine" completed. 65%
complete, about 5.4 minutes to go.

[2020-06-25 19:05:29.056 PDT] PROGRESS: "Manager Upgrade" started. To go -
Phase: 1.1 Total: 5.1 minutes estimate.

[2020-06-25 19:07:47.330 PDT] PROGRESS: "Manager Upgrade" completed. 73%
complete, about 4.4 minutes to go.

[2020-06-25 19:07:47.560 PDT] PROGRESS: "MySql TZ Upgrade" started. To go -
Phase: 2.4 Total: 4.1 minutes estimate.

[2020-06-25 19:10:25.047 PDT] PROGRESS: "MySql TZ Upgrade" completed. 89%
complete, about 1.8 minutes to go.

[2020-06-25 19:10:25.738 PDT] PROGRESS: "Start up Processes" started. To go -
Phase: 1.7 Total: 1.7 minutes estimate.

[2020-06-25 19:13:31.777 PDT] PROGRESS: "Start up Processes" completed. 100%
complete, about 0.0 minutes to go.
```

If you are upgrading a non-persistor node in distributed correlation mode, typical log messages are as follows:

```
[2020-06-25 18:04:01.960 PDT] PROGRESS: "Java Upgrade" started. To go - Phase:
0.4 Total: 2.1 minutes estimate.

[2020-06-25 18:04:08.166 PDT] PROGRESS: "Java Upgrade" completed. 17%
complete, about 0.9 minutes to go.

[2020-06-25 18:04:08.400 PDT] PROGRESS: "Manager Upgrade" started. To go -
Phase: 0.7 Total: 0.7 minutes estimate.

[2020-06-25 18:04:11.607 PDT] PROGRESS: "Manager Upgrade" completed. 100%
complete, about 0.0 minutes to go.
```


Caution: Once you begin the upgrade, you cannot roll back to the previous version of ESM. The uninstallation link does not work with an upgrade. If you encounter errors, ensure that the system tables and log files are available and contact Technical Support. For more information about the items to have available, see Reporting Upgrade Issues.

Upgrading Software ESM in Compact Mode

This section describes how to upgrade software ESM in compact mode. To upgrade software ESM in distributed correlation mode, see Upgrading Software ESM in Distributed Correlation Mode.

To upgrade software ESM in compact mode:

1. As user `arcsight`, untar the `ArcSightESMSuite-7.6.4.xxxx.0.tar` file:

   ```
   tar xvf ArcSightESMSuite-7.6.4.xxxx.0.tar
   ```

2. As user `root`, remove services before running the upgrade:

   ```
   cd <untar_directory>/Tools
   ```

   ```
   ./stop_services.sh
   ```

3. If necessary, upgrade the operating system to a supported version.

   For more information, see the *Technical Requirements* on the ESM documentation page.

4. Services restart after you complete the operating system upgrade and reboot the system. Verify that all services started and are available.

5. As user `arcsight`, run the upgrade:

   ```
   cd <untar_directory>
   ```

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

   Before the upgrade process begins, the upgrade program checks that all upgrade requirements are met. If you encounter an error at this point, correct the error and run the upgrade again.

   If you receive a Java (Manager) heap size error message, press **Enter**. You will need to change the Manager heap size to at least 16 GB after the upgrade. For information about changing the heap size, see Completing Pre-Upgrade Tasks.

   The upgrade performs a pre-upgrade redundant-name check to ensure that your database does not contain duplicate resource names in the same group. If duplicate names exist, the upgrade program generates an error that causes the upgrade to halt. To resolve this error:

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

   b. Resolve duplicate names manually.

   c. Run the upgrade again.

   For assistance, contact Technical Support.

   If the upgrade fails, check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file to determine the point of failure. If your log file *does not* include the following line, correct the error that you find in the log file and run the upgrade again:

   `Pre-upgrade tasks completed successfully.`

   If the upgrade fails at any point after the pre-upgrade checks, contact Technical Support and send all files in the following directories:

```
/opt/arcsight/upgradelogs/
/opt/arcsight/logger/current/arcsight/logger/logs/
/opt/arcsight/var/logs/misc/upgrade/
```

6. Review the information that is provided about the estimated duration of the upgrade and confirm that you want to upgrade your existing ESM installation.

   The upgrade program provides the total estimated duration for completion of the upgrade. If you determine that this is not a convenient time based on the estimated duration, you have the opportunity to cancel the upgrade.

7. Review the information that is provided about overwriting customized content and choose whether to continue the upgrade.

   If you have customized content that you need to back up, see Backing Up Resources Before Upgrading.

8. Specify where to create the link for the installation.
9. Review the settings, select **Install**, and then press **Enter**.
10. If you are running the upgrade in console mode, run the ESM upgrade wizard when prompted:

    ```
    /opt/arcsight/manager/bin/arcsight esmupgradewizard -i console
    ```

    

    Note: If you are running the upgrade in GUI mode, the wizard starts automatically.

11. After the upgrade is complete, as user `root`, run the following script to set up the ArcSight services:

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

12. Hide the obsolete files by running the following:

    ```
    /opt/arcsight/manager/bin/scripts/hide_obsolete_files.sh
    ```

After you run the script to set up the ArcSight services, verify that the upgrade was successful and then complete the applicable post-upgrade tasks. For more information, see Verifying Successful Upgrade and Completing Post-Upgrade Tasks.

After the upgrade completes, ESM starts a process in the background to build case histories into a database table. The case histories are used to display information in the ArcSight Platform. ESM continues to function normally while it builds the case histories. The time to complete building the case histories depends on the volume of cases in the system. To determine whether building of the case histories was successful, check `/opt/arcsight/var/logs/misc/casehistorybuilder.log`. While ESM is building the cases histories, do not shut down ESM. If you need to shut down the Manager before case history

building is complete, after you restart the Manager, run `/opt/arcsight/manager/bin/arcsight buildcasehistory` to restart the process.

After you complete post-upgrade tasks, upgrade the ArcSight Console and Smart Connectors. For more information, see Upgrading the ArcSight Console and Smart Connectors.

Upgrading Software ESM in Distributed Correlation Mode

This section describes how to upgrade software ESM in distributed correlation mode. To upgrade software ESM in compact mode, see Upgrading Software ESM in Compact Mode

To upgrade software ESM in distributed correlation mode:

Note: If you are upgrading ESM in distributed correlation mode and the cluster is also part of an Active Passive High Availability environment, see the Active Passive High Availability Module User's Guide for information about performing the upgrade.

1. On the persistor node, untar the `ArcSightESMSuite-7.6.4.xxxx.0.tar` file:

   ```
   tar xvf ArcSightESMSuite-7.6.4.xxxx.0.tar
   ```

2. On the persistor node, as user `root`, run the following script:

   ```
   cd <untar_directory>/Tools
   ```

   ```
   ./stop_services.sh
   ```

3. On each node *except* the persistor node, complete the following steps:
   a. As user `arcsight`, untar the `ArcSightESMSuite-7.6.4.xxxx.0.tar` file:

      ```
      tar xvf ArcSightESMSuite-7.6.4.xxxx.0.tar
      ```

   b. As user `root`, run the following script:

      ```
      cd <untar_directory>/Tools
      ```

      ```
      ./stop_services.sh
      ```

   c. If necessary, upgrade the operating system to a supported version.

      For more information, see the *Technical Requirements* on the ESM documentation page.

   d. As user `arcsight`, run the upgrade:

      ```
      cd <untar_directory>
      ```

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

e. If you are running the upgrade in console mode, run the ESM upgrade wizard when prompted:

```
/opt/arcsight/manager/bin/arcsight esmupgradewizard -i console
```

Note: If you are running the upgrade in GUI mode, the wizard starts automatically.

f. After the upgrade is complete, as user `root`, run the following script on each cluster node except the persistor node to set up the ArcSight services:

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

g. Hide the obsolete files by running the following:

```
/opt/arcsight/manager/bin/scripts/hide_obsolete_files.sh
```

4. On the persistor node, complete the following steps:

a. If necessary, upgrade the operating system to a supported version.

For more information, see the *Technical Requirements* on the ESM documentation page.

b. As user `arcsight`, run the upgrade:

```
cd <untar_directory>
```

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

c. Review the information that is provided about the estimated duration of the upgrade and confirm that you want to upgrade your existing ESM installation.

The upgrade program provides the estimated duration by upgrade phase and also provides a total estimated duration. The phases are the same as those that are logged in `/opt/arcsight/upgradelogs/suite_upgrade.log`. If you determine that this is not a convenient time based on the estimated duration, you have the opportunity to cancel the upgrade.

Note: The estimated duration is provided only on the persistor node. It is not provided on non-persistor nodes.

d. Review the information that is provided about overwriting customized content and choose whether to continue the upgrade.

If you have customized content that you need to back up, see Backing Up Resources Before Upgrading.

Note: The overwrite message is provided only on the persistor node. It is not provided on non-persistor nodes.

e. If you are running the upgrade in console mode, run the ESM upgrade wizard when prompted:

```
/opt/arcsight/manager/bin/arcsight esmupgradewizard -i console
```

Note: If you are running the upgrade in GUI mode, the wizard starts automatically.

f. After the upgrade is complete, as user `root`, run the following script on the persistor node to set up ArcSight services:

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

g. Hide the obsolete files by running the following:

```
/opt/arcsight/manager/bin/scripts/hide_obsolete_files.sh
```

h. After hiding the obsolete files, delete the following, or older, files manually:

```
/opt/arcsight/logger/current/arcsight/logger/lib/web/htmlunit-1.11.jar
/opt/arcsight/logger/current/arcsight/logger/web/main/WEB-INF/lib/jackson-annotations-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/web/main/WEB-INF/lib/jackson-core-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/web/main/WEB-INF/lib/jackson-databind-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/lib/jackson-annotations-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/lib/jackson-core-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/lib/jackson-databind-2.13.2.jar
/opt/arcsight/logger/current/arcsight/logger/lib/log4j-1.2.13.jar
/opt/arcsight/logger/current/arcsight/logger/web/main/WEB-INF/lib/log4j-1.2.13.jar
/opt/arcsight/logger/current/local/tomcat/webapps/logger/WEB-INF/lib/log4j-1.2.13.jar
/opt/arcsight/logger/current/local/tomcat/webapps/logger/WEB-INF/lib/jackson-annotations-2.10.1.jar
/opt/arcsight/logger/current/local/tomcat/webapps/logger/WEB-INF/lib/jackson-core-2.10.1.jar
/opt/arcsight/logger/current/local/tomcat/webapps/logger/WEB-INF/lib/jackson-databind-2.10.1.jar
/opt/arcsight/logger/current/arcsight/logger/lib/hadoop/slf4j-log4j12-1.7.10.jar
```

i. Once the services are configured, run the following:

```
/opt/arcsight/manager/bin/scripts/prepare_repo.sh
```

5. On each node *except* the persistor node, run the following as an user `acrsight`:

```
/opt/arcsight/manager/bin/scripts/prepare_repo.sh
```

This will prompt you to run the following command on the persistor node to complete the certificate signing for the information repository.

```
/opt/arcsight/manager/bin/scripts/ca_signing.sh
```

6. As user `arcsight`, run the following to stop all the services

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

7. As user `arcsight`, run the following to start all services:

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

After you run the script to set up the ArcSight services, verify that the upgrade was successful and then complete the applicable post-upgrade tasks. For more information, see Verifying Successful Upgrade and Completing Post-Upgrade Tasks.

After the upgrade completes, ESM starts a process in the background on the persistor node to build case histories into a database table. The case histories are used to display information in the ArcSight Platform. ESM continues to function normally while it builds the case histories. The time to complete building the case histories depends on the volume of cases in the system. To determine whether building of the case histories was successful, check `/opt/arcsight/var/logs/misc/casehistorybuilder.log`. While ESM is building the cases histories, do not shut down ESM. If you need to shut down the Manager before case history building is complete, after you restart the Manager, run `/opt/arcsight/manager/bin/arcsight buildcasehistory` to restart the process.

After you complete post-upgrade tasks, upgrade the ArcSight Console and Smart Connectors. For more information, see Upgrading the ArcSight Console and Smart Connectors.

Upgrading ESM on an Appliance

This section describes how to upgrade ESM on an appliance.

Note: If you are upgrading ESM on an appliance that is part of a High Availability environment, see the Active Passive High Availability Module User's Guide for information about performing the upgrade.

Upgrading the Operating System on a B7600 (G9) or B7700 (G10) Appliance

ESM 7.6.4 supports B7600 (G9) and B7700 (G10) appliances running on RHEL 7.9.

If you are running ESM 7.2 on a G9 or G10 appliance that is running RHEL 7.7, you must first upgrade the operating system to RHEL 7.8 and upgrade ESM to ESM 7.3. Then, you must upgrade the operating system to RHEL 7.9 and upgrade ESM to ESM 7.5. After you complete the required operating system and ESM upgrades, you can upgrade to ESM 7.6.

Even if you previously upgraded the operating system to the supported version, Micro Focus recommends upgrading the operating system with each release, using the upgrade script for the current release. This upgrade script provides security and other important updates.

To upgrade from RHEL 7.7 to RHEL 7.9 on a B7600 (G9) or B7700 (G10) appliance:

1. As user `root`, download the upgrade file:

   `esm_osupgrade_rhel79_20211129221711.tar.gz`

   Micro Focus provides a digital public key to enable you to verify that the signed software that you received is from Micro Focus and has not been manipulated by a third party. For more information and instructions, visit the Signature Verification page.

   To initiate license procurement, after you download the `.tar` file, follow the instructions in the Electronic Delivery Receipt that you receive in e-mail.
2. From the directory where you downloaded the upgrade file, extract the file:

   ```
   /bin/tar zxvf esm_osupgrade_rhel79_20211129221711.tar.gz
   ```
3. Change directory:

   ```
   cd esm-rhel79upgrade
   ```
4. Run the following command:

   ```
   chmod 0700 osupgrade
   ```
5. Run the following command to start the operating system upgrade and generate an upgrade log file:

   ```
   /osupgrade 2>&1 | tee osupgrade.log
   ```

   When the operating system upgrade completes, the system reboots and services restart. Before you continue with the upgrade to ESM 7.6, verify that all services are available.
6. Run the following command to verify the operating system version:

```
cat /etc/redhat-release
```

The result should be `Red Hat Enterprise Linux Server release 7.9`.

Upgrading the Appliance to ESM 7.6.4

After you complete any required operating system upgrades, upgrade the appliance to ESM 7.6.

To upgrade the appliance:

1. Log in as user `arcsight`.
2. If you did not perform an operating system upgrade, download the appropriate operating system upgrade script for your appliance. The scripts include an entropy generator, `rng-tools`, that you will need to run if you encounter entropy errors during the upgrade. ESM requires high levels of operating system entropy for secure cryptography.

   To upgrade a B7600 (G9) or B7700 (G10) appliance, download `esm_osupgrade_rhel79_20211129221711.tar.gz`.
3. You can perform the remaining steps directly on the appliance or remotely using ssh. To use ssh, open a shell window:

   ```
   ssh root@<hostname>.<domain>
   ```
4. Change to the directory where you downloaded the upgrade files.
5. Untar the `ArcSightESMSuite-7.6.0.xxxx.0.tar` file:

   ```
   tar xvf ArcSightESMSuite-7.6.4.xxxx.0.tar
   ```
6. As user `root`, remove services before running the upgrade:

   ```
   cd <untar_directory>/Tools
   ```

   ```
   ./stop_services.sh
   ```
7. As user `arcsight`, run the upgrade:

   ```
   cd <untar directory>
   ```

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

   Before the upgrade process begins, the upgrade program checks that all upgrade requirements are met. If you encounter an error at this point, correct the error and run the upgrade again.

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

Before the upgrade process begins, the existing software components will be backed up to the following locations:

`/opt/arcsight/manager.preUpgradeBackup`

`/opt/arcsight/logger/BLxxxx`

Services are backed up to `/opt/arcsight/services.preUpgradeBackup`. The suite is backed up to `suite.preUpgradeBackup`. System tables are exported to `/opt/arcsight/manager.preUpgradeBackup/tmp/arcsight_dump_system_tables.sql.<timestamp>` and user sequences are exported to `/opt/arcsight/manager.preUpgradeBackup/tmp/user_sequences_backup.sql`.

Do not delete the backup files before the upgrade is complete and you verify that it was successful. You might need the backup files to recover the system in case of a failed upgrade.

If you receive a Java (Manager) heap size error message, press **Enter**. You will need to change the Manager heap size to at least 16 GB after the upgrade. For information about changing the heap size, see Completing Pre-Upgrade Tasks.

If the upgrade fails, check the `/opt/arcsight/upgradelogs/suite_upgrade.log` file to determine the point of failure. If your log file *does not* include the following line, correct the error that you find in the log file and run the upgrade again:

`Pre-upgrade tasks completed successfully.`

If the upgrade fails at any point after the pre-upgrade checks, contact Technical Support and send all files in `/opt/arcsight/upgradelogs/`.

8. Review the information that is provided about overwriting customized content and choose whether to continue the upgrade.

   If you have customized content that you need to back up, see Backing Up Resources Before Upgrading.

9. After the Manager upgrade completes, check the upgrade summary report in `/opt/arcsight/manager/upgrade/out/<timestamp>/summary.html`.

10. After the upgrade is complete, as user `root`, run the following script to set up the ArcSight services:

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

After you run the script to set up the ArcSight services, verify that the upgrade was successful and then complete the applicable post-upgrade tasks. For more information, see Verifying Successful Upgrade and Completing Post-Upgrade Tasks.

After the upgrade completes, ESM starts a process in the background to build case histories into a database table. The case histories are used to display information in the ArcSight Platform. ESM continues to function normally while it builds the case histories. The time to complete building the case histories depends on the volume of cases in the system. To

determine whether building of the case histories was successful, check `/opt/arcsight/var/logs/misc/casehistorybuilder.log`. While ESM is building the cases histories, do not shut down ESM. If you need to shut down the Manager before case history building is complete, after you restart the Manager, run `/opt/arcsight/manager/bin/arcsight buildcasehistory` to restart the process.

After you complete post-upgrade tasks, upgrade the ArcSight Console and Smart Connectors. For more information, see Upgrading the ArcSight Console and Smart Connectors.

Upgrading a Hierarchical or Other Multi-ESM Installation

This chapter describes the method for upgrading a multi-ESM deployment to ESM 7.6.4.

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 that connect to them, followed by the standby or source ESMs. Upgrade ArcSightForwarding Connectors only *after* you upgrade their corresponding source/destination ESMs. The Forwarding Connectors must be the version that shipped with ESM, or the latest version.

To upgrade a hierarchical deployment:

Note: Start with the top-tier ESM and repeat these steps for each level of the hierarchy.

1. Upgrade any SmartConnectors that are not running the latest version.

   For more information, see the SmartConnector User Guide.
2. Remove the ArcSight services on the current ESM.
3. Follow the instructions in Running the Upgrade.
4. After the ESM upgrade is complete and you have completed the applicable post-upgrade tasks, upgrade the ArcSight Console.

For more information, see Completing Post-Upgrade Tasks and Upgrading the ArcSight Console and Smart Connectors.

5. Upgrade the Forwarding Connector. For complete instructions, see the ArcSight Forwarding Connector Configuration Guide.

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

   The Forwarding Connector must be the version that shipped with ESM.

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

Verifying Successful Upgrade

This section describes how to ensure that the upgrade was successful.

To verify successful upgrade:

1. Check the upgrade summary report and logs to determine whether the ArcSight Manager was successfully upgraded. The upgrade summary report (`<ARCSIGHT_HOME>/upgrade/out/<timestamp>/summary.html`) is only applicable to the Manager.

   Note: You might see a message similar to `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 that some tables were not upgraded due to missing meta data. This condition should not affect existing functionality.

2. Verify that the `/opt/arcsight/upgradelogs/suite_upgrade.log` file includes an `Upgrade completed successfully` message.
3. Run the following command to verify the build versions:

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

   The response should be similar to the following:

   ```
   Build versions:
   esm: 7.6.4.2728.0(BE2728)
   storage: 7.6.4.2063.0(BL2063)
   process management: 7.6.0-2522
   installer: 7.6.4-2522
   ```

4. Run the following command to verify that all components are available:

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

The response should be 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
```

Reporting Upgrade Issues

If you encounter issues during the upgrade, ensure that the necessary items are available and contact Technical Support. Be prepared to provide the following items:

- System tables located in `/opt/arcsight/manager.preUpgradeBackup/tmp/arcsight_dump_system_tables.sql.<timestamp>`
- Suite upgrade logs:
  - `/opt/arcsight/upgradelogs/suite_upgrade.log`

    This log provides an overview of the upgrade progress and is the first log that you should consult in the event that your upgrade fails.
  - `/home/arcsight/ArcSight_ESM_7.6.4.0_Suite_Install_<timestamp>.log`
- Logger upgrade logs:
  - `/opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log`
  - `/opt/arcsight/logger/current/arcsight/logger/logs/initmysqluser.log`
  - `/opt/arcsight/logger/current/arcsight/logger/logs/postgressql_upgrade.out`
  - `/opt/arcsight/logger/userdata/logger/logs/mysql5.7upgrade.log`
- ArcSight Manager upgrade logs:
  - `/opt/arcsight/manager/upgrade/out/<timestamp>/logs/upgrade/server.upgrade.log`
  - `/opt/arcsight/manager/upgrade/out/<timestamp>/logs/upgrade/server.upgrade.std.log`
- `/opt/arcsight/services/logs/arcsight_services.log` (ArcSight services upgrade log)
- Installation logs:
  - `/home/arcsight/ArcSight_ESM_7.6.4.0_Suite_Install_<timestamp>.log`

- /home/arcsight/ArcSight_Logger_7.6.4.0_Install_<timestamp>.log
- /home/arcsight/ArcSight_ESM_Manager_7.6.4.0_Install_<timestamp>.log

Chapter 3: Completing Post-Upgrade Tasks

After you have confirmed that the upgrade was successful, complete the applicable tasks in this section. For information about required tasks, see Completing Required Post-Upgrade Tasks. For information about optional tasks, see Completing Optional Post-Upgrade Tasks.

After you complete the applicable post-upgrade tasks, upgrade the ArcSight Console and Smart Connectors. For more information, see Upgrading the ArcSight Console and Smart Connectors.

Completing Required Post-Upgrade Tasks

This section describes tasks that you must complete after you verify that the upgrade was successful.

Note: Depending on your configuration, some tasks might not be applicable.

To complete required post-upgrade tasks:

1. If you upgraded software ESM and did not install the time zone update package before you upgraded or did not install it when prompted during the upgrade, you must install it now.

   ESM uses the time zone update package to automatically handle changes in time zone or changing between standard and daylight savings time.

   For information about installing the time zone update package, see Software ESM: Installing the Time Zone Package.

2. Correct invalid resources.

   You checked for invalid resources before the upgrade. It is possible that during upgrade, the condition statement for a resource that you created or modified became invalid. For example, if the schema of an ESM-supplied active list changed and a resource that 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. Review the upgrade summary report at `</opt/arcsight/manager/upgrade/out/<timestamp>/summary.html` to identify invalid resources and correct their conditions.

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

   For information about running the resource validator, see Running the Resource Validator.

3. Delete unassigned `.art` files.

   The upgrade might result in unassigned resources. For example, `.art` files are created as new file resources in ESM, and the upgrade assigns new version IDs to these resources. The original files are stored in the **Files** resource in the **Unassigned** folder.

   Because they are duplicates, you can safely delete the unassigned `.art` files.

4. Restore or delete deprecated resources.

   For more information, see Restoring or Deleting Deprecated Resources.

5. Restore custom Velocity templates.

   The upgrade adds a `.previous` file extension to preserve customized velocity templates and replaces the original file with an un-customized version. To restore your customized version, delete the new file and remove the `.previous` file extension from your customized version.

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

6. Update the Cases user interface.

   For more information, see Updating the Cases User Interface.

7. Restore and verify customized standard resources.

   For more information, see Restoring and Verifying Customized Standard Resources.

8. Remove deprecated Threat Response Manager (TRM) integration commands.

   The TRM integration commands are deprecated and should not be used. Delete the following folders to remove the TRM integration commands from the **Integration Commands** menu:

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

9. To facilitate proper data collection, re-register any connectors that support IPv6 addresses.
10. Verify that the upgrade program successfully transferred your content to the upgraded structures.

    For more information, see Verifying Content Transfer.

11. If you previously linked assets to default system zones, the assets might have lost the zone information. Micro Focus does not recommend linking assets to default system zones. Create custom zones (including configuring the category) and link the assets to the new custom zones.

For information about creating customized zones, see the ArcSight Console User's Guide.

12. If you are upgrading to ESM version 7.6 from distributed mode, complete the following steps:
    a. In ArcSight Command Center, open the Cluster View dashboard.
    b. Under **Backpressure**, ensure that the **Acceptable Lag** setting is not less than 300 seconds.
13. If you are in distributed correlation mode, to facilitate JMX authentication, restart all `repo` instances.

After you complete the required upgrade tasks, continue to Completing Optional Post-Upgrade Tasks. If the optional tasks do not apply to your configuration, continue to Upgrading the ArcSight Console and Smart Connectors.

Restoring or Deleting Deprecated Resources

Some resources and resource groups have been deprecated, meaning they are no longer needed. Resources are deprecated for the following 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 features accomplish the same goal more efficiently.

The upgrade program moved deprecated resources to a separate `Deprecated` group for that resource type. The resources retain the hierarchy from the previous ESM version. These resources remain active so that they will be present and operational if you rely on them.

Note: If you built resources that refer to a deprecated resource, or if you modified a deprecated resource to refer to a resource that has not been deprecated, some connections might break during the upgrade.

If you still need to use the deprecated resource, move the deprecated resource back to the active resource tree and change the conditions as needed.

If you choose to restore a deprecated resource, you are responsible for its maintenance. Verify whether new resources address the same goal more efficiently.

For example, if the upgrade program moved `/All Rules/Arcsight System` to `/All Rules/Arcsight System/Deprecated` and you plan to continue using the resource, move it to your own group after the upgrade is complete.

To generate a list of deprecated resources:

1. In the ArcSight Console, select **Edit > Find Resource**.
2. In the search field, enter the keyword **deprecated** and press **Enter**.

Updating the Cases User Interface

Complete this task before you upgrade the ArcSight Console.

If you *did not* customize the Cases user interface, at a minimum you must rename an XML file that the upgrade program provided to ensure that you receive updates pertaining to the user interface structure (for example, new fields).

If you customized the Cases user interface in a previous ESM version, you must manually restore the customized files so that you can continue using those customizations and also access new Cases editor fields.

To update the Cases user interface if you did not previously customize it:

1. In `/opt/arcsight/manager/config/`, rename `caseui.xml` to `caseui.xml.old`.
2. Locate `caseui.xml.orig` (the file that the upgrade program provided) and rename it to `caseui.xml`.
3. Stop the ArcSight Manager:

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

4. Start the services to implement the upgraded Cases user interface structure and expose any new fields:

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

The updates are propagated to both ArcSight Command Center and the ArcSight Console.

To update the Cases user interface if you previously customized it:

1. In `/opt/arcsight/manager.preUpgradeBackup/i18n/common`, locate the properties files that you customized (for example, `label_strings_en.properties` and `resource_strings_en.properties`, and other localized properties files).

   The upgrade process installs the latest properties files in `/opt/arcsight/manager/i18n/common`.
2. Open one of the customized properties files (for example, `/opt/arcsight/manager.preUpgradeBackup/i18n/common/label_strings_<*Locale*>.properties`) and locate your customizations.

Tip: Search for the string `extendedcase` to locate your customized field labels.

3. Copy the customizations to the corresponding properties file that the upgrade program provided (located in `/opt/arcsight/manager/i18n/common/`).

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

   After you upgrade the ArcSight Console (Upgrading the ArcSight Console and Smart Connectors), copy the following customized files to the individual Console installations at `arcsight\console\i18n\common\`:

   - `label_strings`
   - `resource_strings`

4. In `/opt/arcsight/manager/config/`, rename `caseui.xml` to `caseui.xml.old`.
5. If you changed the user interface structure, in `/opt/arcsight/manager.preUpgradeBackup/config`, open the customized copy of `caseui.xml` and locate your customizations.
6. Copy your customizations to `caseui.xml.orig` (in `/opt/arcsight/manager/config/`).
7. Rename `caseui.xml.orig` to `caseui.xml`.
8. If there is a customized case details mapping to audit events, copy `case.properties` from `/opt/arcsight/manager.preUpgradeBackup/config/audit` to `/opt/arcsight/manager/config/audit`.
9. Stop the ArcSight Manager:

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

10. Start the services:

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

Restoring and Verifying Customized Standard Resources

If you created a `.arb` file in the topic Preparing Resources for Upgrade, import it and verify that its contents work as expected.

Updates to standard content that occurred during the upgrade might cause resources that you created to work in a way that you did not intend. For example, a rule might trigger too often or not at all if it uses a filter in which conditions were changed.

To verify that resources that you created work as expected:

1. Send events that you know will trigger the content using the Replay with Rules feature.

   For more about this feature, see the ArcSight Console User's Guide.
2. Check the Live or All Events active channel to verify that the correlation event was triggered. Ensure that the data monitors that you created return the expected output based on the test events that you sent.
3. Verify that notifications were sent to the recipients in your notification destinations.
4. Verify that active lists that you created to support your content gather the replay with rules data.
5. During the upgrade process, the resource validator identified resources that were rendered invalid (conditions that no longer work) during the upgrade. Identify invalid resources and correct their conditions as appropriate.

Verifying Content Transfer

After the upgrade is complete, verify that the upgrade program transferred your content to the upgraded structures.

Note: The upgrade program imports packages but does not install them, even if they are mandatory. You must manually install packages after the upgrade program imports them. Packages that you installed before the upgrade remain installed.

To verify content transfer:

1. For all resource types, check for resources in the **Unassigned** group in the resource tree. If resources are present, move them to the appropriate custom group.

   Unassigned groups contain resources that you created and were previously located in the **System** group.

   Note: Micro Focus recommends that you do not move these resources to standard content groups. Future upgrades will move the resources back to the **Unassigned** group.
2. Check for assets in the **Disabled** group.

   The **Disabled** group in the assets resource tree queries the ArcSight Manager every two minutes for assets that have been disabled. If you find assets in the **Disabled** group, review the disabled assets to determine why they were disabled and make the appropriate corrections. 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.

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. This might occur for assets that use the fully-qualified domain dame (FQDN) of the asset as the host name. When comparing the two assets, only the host name is extracted from the FQDN.

For example, if two assets have FQDNs `myhost.mycompany.com` and `myhost.mycompany.us.com`, ESM only uses the value `myhost` to compare them. Since the host name is identical, these two assets are considered conflicting assets and one of them becomes invalid. To override this behavior and use the FQDN instead, set the following property in the `server.properties` file:

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

You can delete disabled assets if you no longer need them.

3. Verify that access control lists are correct and valid based on the organization of the standard content.

   For example, only users with authority to work with system-level content such as `ArcSight System` and `ArcSight Administration` should have Administrator access.

4. Check for invalid zones:
   a. Correct zones that you want to retain and delete zones that you do not want to retain.
   b. Verify that assets that are assigned to zones that were moved or invalidated during the upgrade retain connections to appropriate zones.
   c. If you customized existing standard zones, edit the new resource to restore the customizations. Do not import the old zone.

Completing Optional Post-Upgrade Tasks

This section describes optional post-upgrade tasks. Ensure that the upgrade was successful before you perform these tasks.

To complete optional post-upgrade tasks:

1. Archive backup files that the upgrade program created.

   The upgrade program creates backup files for rollback purposes. These files might contain outdated JREs and other components that include vulnerabilities. Security scanners can detect these vulnerabilities. To avoid issues with security scanners, you can archive these backup files and restore them if necessary.

   To archive the backup files, run the following script:

   ```
   opt/arcsight/manager/bin/arcsight hide_obsolete_files
   ```

The archive is created in `/opt/arcsight`. You can relocate the archive, but you must move it back to `/opt/arcsight` in order to restore it.

If you need to revert to the previous version of ESM for any reason, you must restore the archive first. To restore the archive, run the following script:

```
opt/arcsight/manager/bin/arcsight hide_obsolete_files -u <archive name>
```

For example, `opt/arcsight/manager/bin/arcsight hide_obsolete_files -u BLXXXX`.

2. Convert from compact mode to distributed correlation mode.

   For more information, see Converting from Compact Mode to Distributed Correlation Mode.

3. Convert appliances to prefer IPv6.

   For more information, see Appliance: Converting to Prefer IPv6.

4. Install the following packages:

   - ArcSight SocView
   - ArcSight ClusterView
   - Threat Intelligence Platform
   - Security Threat Monitoring
   - ArcSight ESM SOAR Integration

   For descriptions of these packages, see the ArcSight Administration and ArcSight System Standard Content Guide.

   ESM automatically installs content packages for new installations. However, when you upgrade, new packages are not automatically installed. You can install these packages from the ArcSight Console after the upgrade.

   For information about installing these packages, see the ArcSight Console User's Guide.

5. Install NetFlow SmartConnectors.

   NetFlow events from the following SmartConnectors trigger NetFlow Monitoring content:

   - ArcSight IP Flow SmartConnector
   - ArcSight QoSient ARGUS SmartConnector

   These SmartConnectors are not installed with ESM. To use the NetFlow Monitoring content, install and configure these SmartConnectors. For information about obtaining the SmartConnectors, contact your sales representative.

6. Install the ArcSight Platform.

The ArcSight Platform enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment:

- Real-time event monitoring and correlation with data from ESM
- Analyzing end-user behavior with Interset

To help you get started, the ArcSight Platform provides a Dashboard with a set of out-of-the-box widgets and dashboards. Users can organize the widgets into personalized dashboards.

For information about deploying, configuring, and maintaining this product, see the Release Notes and the Administrator's Guide for the ArcSight Platform.

Note: This release allows you to connect to a single ESM instance.

7. If you want the ability to view Command Center from the ArcSight Platform, install ESM in the ArcSight Platform and then configure the ESM host in the ArcSight Platform. For more information, see the Administrator's Guide for the ArcSight Platform.

   This feature allows you to view Command Center from the ArcSight Platform without having to switch to the ESM host for Command Center. After you install ESM and configure the host in the ArcSight Platform, refresh the dashboard to display the Command Center menu in the ArcSight Platform. Click the menu to start Command Center. To go back to the ArcSight Platform dashboard from Command Center, use the ArcSight Platform menu from the Dashboard menu in Command Center.
8. Configure Recon access.

   For more information, see Configuring Recon Access.
9. Configure Transformation Hub access.

   For more information, see the applicable topic:

   - Configuring Transformation Hub Access - Non-FIPS Mode
   - Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode
   - Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)
10. Configure integration with ServiceNow® IT Service Management (ITSM).

    For more information, see Configuring Integration with ServiceNow® IT Service Management (ITSM).

After you complete optional post-upgrade tasks, continue to Upgrading the ArcSight Console and Smart Connectors.

Converting from Compact Mode to Distributed Correlation Mode

If you previously installed ESM in compact mode, you can convert the system to distributed correlation mode.

It is important to plan the cluster before you convert your system. For information about cluster planning, see the ESM Installation Guide.

Before you start the conversion process, you must ensure that information repository instances will not run on the disk partition that contains `/opt/arcsight`. In a distributed correlation environment, running an information repository instance on the disk partition that contains `/opt/arcsight` leads to performance problems. To avoid these problems, you must create `/var/opt/arcsight` (as a directory or a symbolic link to a directory) on all of the cluster nodes before you upgrade ESM. If `/var/opt/arcsight` does not meet the requirements that are listed below, the upgrade program will generate an error and will not continue. During the upgrade, the upgrade program moves repository data to the partition that contains `/var/opt/arcsight`.

The `/var/opt/arcsight` directory (or the directory that it points to) must meet the following requirements:

- `/var/opt/arcsight` must not be in the same partition that contains `/opt/arcsight`.
- The `arcsight` user must own the directory.
- The partition that contains `/var/opt/arcsight` must have at least 1 GB of free disk space.

Note: To convert from compact mode to distributed correlation mode, each server host name must resolve to an IP address for each cluster node. Otherwise, the conversion process will fail with an error message.

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 to the `arcsight` user.
3. Stop the ArcSight Manager:

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

4. Change directory to `/opt/arcsight/manager`.
5. Initialize distributed correlation mode:

   ```
   bin/arcsight initialize-distributed-mode
   ```

6. Set up the information repository, using the option **Change the TCP Port Range for ESM Processes** to specify the port range:

   ```
   bin/arcsight reposetup
   ```

   For more information about `reposetup`, see the ESM Administrator's Guide.

7. Run `managersetup`:

   ```
   bin/arcsight managersetup
   ```

   For more information about `managersetup`, see the ESM Administrator's Guide.

   Important: Do not start the ArcSight Manager after `managersetup` is complete.

8. Initialize certificate administration and create a password for certificate administration:

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

   For information about password restrictions, see the ESM Administrator's Guide.

9. Add the version information for this node:

   ```
   /etc/init.d/arcsight_services setLocalBuildVersions
   ```

10. If you need a distributed cache instance on the persistor node, run the following command:

    ```
    bin/arcsight dcachesetup
    ```

    For more information about `dcachesetup`, see the ESM Administrator's Guide.

11. Add correlators or aggregators as needed on the persistor node:

    ```
    bin/arcsight correlationsetup
    ```

    For more information about `correlationsetup`, see the ESM Administrator's Guide.

The system is now in distributed correlation mode. For information about installing ESM on the remaining cluster nodes, see the ESM Installation Guide.

To complete configuration and bring up the services:

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

1. Set up passwordless SSH:

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

2. Review and approve all certificates:

```
bin/arcsight certadmin -list submitted
```

Review the output to verify that the certificates represent the nodes where the ArcSight Manager or correlation services were installed. To view the certificate details, use the `-v` option.

3. After you confirm that the certificate list is correct, run the following command:

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

4. Stop all services:

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

5. Start the repository service:

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

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

```
bin/arcsight mbussetup
```

For more information about `mbussetup`, see the ESM Administrator's Guide.

7. If you need additional repository instances, run the following command:

```
bin/arcsight reposetup
```

For more information about `reposetup`, see the ESM Administrator's Guide.

8. Start all services, which will bring up services related to distributed correlation mode:

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

9. Verify that all services are running:

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

Appliance: Converting to Prefer IPv6

After the upgrade, you can convert your ESM appliance to a pure IPv6 network configuration and convert ESM to prefer using IPv6, or convert the appliance to a dual stack configuration.

Note: You will need to re-register any connectors that are registered on the appliance after you complete the conversion. The IPv4 IP address will change to a host name and the ArcSight Manager certificate will be regenerated.

To convert an appliance to use IPv6:

1. As user root or arcsight, stop all services:

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

2. As user root or arcsight, confirm that all services are stopped:

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

3. As user root, run the network configuration script and select **IPv6** or **Dual Stack** to change the operating system:

   ```
   /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. As user root, stop the Manager service:

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

7. As user arcsight, run managersetup again:

   ```
   /opt/arcsight/manager/bin/arcsight managersetup
   ```

8. Change the preferred IP protocol to IPv6 and change the host name to the host name of the appliance's IPv6 address.
9. Regenerate the ArcSight Manager certificate.
10. As user root, start the ArcSight Manager:

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

Configuring Recon Access

This section describes how to configure ESM to access Recon.

Note: ESM 7.6 requires Recon 1.1.0.

To configure ESM access to Recon:

1. As user arcsight, stop the ArcSight Manager services:

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

2. As user `arcsight`, from the `/opt/arcsight/manager/bin` directory, start the `managersetup` wizard:

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

   Advance through the wizard until you reach the Recon screen.
3. Specify the search URL for the Recon deployment.
4. Advance through the wizard and complete the configuration.

   For more information about `managersetup`, see the ESM Administrator's Guide.
5. As user `arcsight`, restart the ArcSight Manager:

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

Configuring Transformation Hub Access - Non-FIPS Mode

This section describes how to configure ESM to access Transformation Hub when FIPS mode is *not* enabled.

To configure ESM access to Transformation Hub in non-FIPS mode:

1. As user `arcsight`, stop the ArcSight Manager:

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

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

   Advance through the wizard until you reach the Transformation Hub screen.
3. Provide the following information:
   a. Specify the host name or IP address and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

      Note: You must specify the host name and *not* the IP address.

      Transformation Hub can only accept IPv4 connections from ESM.

      If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

   b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

For more information, see the Administrator's Guide for the ArcSight Platform.

Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2).

c. Import the Transformation Hub root certificate to ESM's client truststore.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

Copy the Transformation Hub root certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` on the Transformation Hub server to a local folder on the ESM server. After you provide the path to the certificate, the wizard imports the Transformation Hub root certificate into ESM's client truststore.

d. If the Kafka cluster is not configured to use SASL/PLAIN authentication, leave the authentication type as None. If the Kafka cluster is configured to use SASL/PLAIN authentication, select SASL/PLAIN as the authentication type.

e. If you selected SASL/PLAIN as the client authentication type, specify the user name and password for authenticating to Kafka.

The wizard validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

4. Advance through the wizard and complete the configuration.

For more information about `managersetup`, see the ESM Administrator's Guide.

5. As user `arcsight`, restart the ArcSight Manager:

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

6. To verify that the connection to Transformation Hub is working, look for the line `Transformation Hub service is initialized` in `server.std.log`.

Setting Up SSL Client-Side Authentication Between Transformation Hub and ESM - Non-FIPS Mode

Before setting up client-side authentication with Transformation Hub, you must import the Transformation Hub root certificate into the ESM truststore.

Transformation Hub maintains its own certificate authority (CA) to issue certificates for individual nodes in the Transformation Hub cluster. ESM needs that CA certificate in its truststore so that it will trust connections to Transformation Hub. For information about obtaining the certificate, see the information about viewing and changing the certificate authority in the Administrator's Guide for the ArcSight Platform. You might need to contact the Transformation Hub administrator to obtain the CA certificate if you do not have sufficient privileges to access the Transformation Hub cluster.

To import the Transformation Hub root certificate into the ESM truststore:

Note: Before completing the steps below, verify whether the Transformation Hub root certificate has previously been imported into ESM. If it has, you do not need to re-import it.

1. On the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
2. Use the `keytool` command to import the root CA certificate into the ESM 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.crt
   ```

To enable client-side authentication between Transformation Hub and ESM:

1. Obtain your company's root CA certificate, an intermediate certificate, and key pair and place them in `/tmp` with the following names:
   - `/tmp/intermediate.cert.pem`
   - `/tmp/intermediate.key.pem`
   - `/tmp/ca.cert.pem`
2. Verify that Transformation Hub is functional and that client authentication is configured.
3. As user `arcsight`, stop the ArcSight 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.
6. Run the following commands to update the empty password of the generated key `services-cn` in the keystore to be the same password as that of the keystore itself:

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

   When prompted, enter the same password that you entered for the store password:

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

7. Run the following command to update the password in `config/client.properties`:

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

8. Generate the keypair and certificate signing request (`.csr`) file. When generating the keypair, enter the fully-qualified domain name of the ArcSight Manager host as the common name (CN) for the certificate.

   Run the following 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

9. Sign the `.csr` with the Transformation Hub root certificate. On the Transformation Hub server, the root certificate is located at `/opt/arcsight/kubernetes/ssl/intermedite.cert.pem` and the key is called `ca.key`.

   Run the following command on either the Transformation Hub server or a different server with a functional `openssl` (as long as you have the `intermediate.cert.pem` and `intermediate.key.pem` available):

   ```
   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 storing
   the 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
```

You must specify all file locations with the full path.

10. Import the intermediate certificate from Transformation Hub 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
```

11. On the ESM server, run the following command to import the signed certificate (the `-out` parameter in the above `openssl` 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
```

12. To verify that the configuration is complete and that the connection to Transformation Hub is valid, run `managersetup` and ensure that there are no errors.
13. Start the ArcSight Manager:

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

Configuring Transformation Hub Access - FIPS Mode (Server Authentication Only)

This section describes how to configure ESM to access Transformation Hub when FIPS mode is enabled. FIPS 140-2 is the only supported FIPS mode.

To configure ESM access to Transformation Hub in FIPS Mode:

1. As user `arcsight`, stop the ArcSight Manager:

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

2. From the Transformation Hub server, copy the certificate from `/opt/arcsight/kubernetes/scripts/cdf-updateRE.sh > /tmp/ca.crt` to a location on the ESM server.
3. Use the `keytool` command to import the root CA certificate into the ESM client truststore:

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

4. As user `arcsight`, run the following command from the `/opt/arcsight/manager/bin` directory to start the `managersetup` wizard:

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

5. Provide the following information:

Note: You do not need to provide the path to the Transformation Hub root certificate, as it has already been imported.

   a. Specify the host name or IP address and port information for the nodes in Transformation Hub. Include the host and port information for all nodes and not just the master node. Use a comma-separated list (for example: <host>:<port>,<host>:<port>).

Note: You must specify the host name and *not* the IP address.

Transformation Hub can only accept IPv4 connections from ESM.

If the Kafka cluster is configured to use SASL/PLAIN authentication, ensure that you specify the port configured in the cluster for the SASL_SSL listener.

   b. Specify the topics in Transformation Hub from which you want to read. These topics determine the data source.

   For more information, see the Administrator's Guide for the ArcSight Platform.

Note: You can specify up to 25 topics using a comma-separated list (for example: topic1,topic2).

   c. If the Kafka cluster is not configured to use SASL/PLAIN authentication, leave the authentication type as None. If the Kafka cluster is configured to use SASL/PLAIN authentication, select SASL/PLAIN as the authentication type.

   d. If you selected SASL/PLAIN as the client authentication type, specify the user name and password for authenticating to Kafka.

The wizard validates the connection to Transformation Hub. If there are any issues, you will receive an error or warning message. If the wizard does not generate error or warning messages and you are able to advance to the next screen, the connection is valid.

6. Advance through the wizard and complete the configuration.

   For more information about `managersetup`, see the ESM Administrator's Guide.

7. As user `arcsight`, restart the ArcSight Manager:

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

8. To verify that the connection to Transformation Hub is working, look for the line `Transformation Hub service is initialized` in `server.std.log`.

Configuring Integration with ServiceNow® IT Service Management (ITSM)

This section describes how to integrate with ServiceNow® IT Service Management (ITSM) after completing the upgrade.

To configure ESM to integrate with ServiceNow® ITSM:

1. As user `arcsight`, stop the ArcSight Manager services:

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

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

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

   Advance through the wizard until you reach the ServiceNow® ITSM screen.

3. Specify the ServiceNow® URL and, optionally, the ServiceNow® proxy URL.
4. If you want to use a global ID to authenticate connections to ServiceNow, click **Yes**, and then specify the user name and password.
5. Advance through the wizard and complete the configuration.

   For more information about `managersetup`, see the ESM Administrator's Guide.

6. As user `arcsight`, restart the ArcSight Manager:

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

Chapter 4: Upgrading the ArcSight Console and Smart Connectors

After you complete the ESM upgrade process and complete post-upgrade tasks, upgrade the ArcSight Console and SmartConnectors.

Upgrading the ArcSight Console

Before you upgrade the console, complete the applicable upgrade process in Running the Upgrade and the applicable post-upgrade tasks in Completing Post-Upgrade Tasks. You must upgrade all ArcSight Console instances that connect to the ArcSight Manager that is running on the upgraded system.

Note: Starting with ESM 7.0 Patch 1, the Event Reconciliation and Session Reconciliation data monitors are deprecated. If you created any of these data monitors, they will not function after the upgrade. In the resource navigator, the resources will appear as invalid.

To upgrade the ArcSight Console:

1. Download the appropriate installation file for your platform from the Licensing and Downloads site (where xxxx in the file name represents the build number) and transfer it to the location where you plan to install the console:
   - `ArcSight-7.6.0.xxxx.0-Console-Win.exe`
   - `ArcSight-7.6.0.xxxx.0-Console-Linux.bin`
   - `ArcSight-7.6.0.xxxx.0-Console-MacOSX.zip`
2. Stop the ArcSight Console.
3. Run the appropriate installation file:
   - On Windows, double-click `ArcSight-7.6.0.xxxx.0-Console-Win.exe`.
   - On Macintosh, unzip `ArcSight-7.6.0.xxxx.0-Console-MacOSX.zip` and then double-click the installation program.

     Note: The installation program does not import the certificate. After the upgrade is complete, you will be prompted to import the certificate when you connect to the ArcSight Manager. Click **OK**, and the console completes the import.
   - On Linux, run the following command as a non-root user:

     ```
     ./ArcSight-7.6.0.xxxx.0-Console-Linux.bin
     ```

To install in console mode, run the following command from the shell prompt:

```
./ArcSight-7.6.0.xxxx.0-Console-Linux.bin -i console
```

4. Follow the prompts to complete the installation.

   When the installation program prompts you to choose an installation folder, specify an `<ARCSIGHT_HOME>` path that is *not* in the same location as the existing ArcSight Console. Choosing a different location prevents the installation program from overwriting your existing configuration so that you can migrate settings from it later.

   The installation program prompts you for a previous installation and provides the option to copy settings to the new console. These settings include the ArcSight Manager host name or IP address and port number and authentication information. Select to transfer these settings.

   When the installation program prompts you to select an IP protocol, select the protocol that corresponds to your ESM server configuration.

When the installation program is complete, you must configure the console. For information about configuration tasks, see the ESM Installation Guide.

If you previously customized any field labels in the Cases user interface, see Updating the Cases User Interface for instructions on what to do with the label properties files.

After you complete the upgrade and configure the console, verify the following:

- You can view the upgraded standard content.
- Customized Cases user interface labels display correctly.
- SmartConnectors are connected to the ArcSight Manager and the Manager is receiving events from them.

  If event viewers do not appear initially, select the `/All Active Channels/ArcSight System/Core/Live` channel to view real-time events.

Upgrading ArcSight SmartConnectors

MicroFocus recommends that you upgrade all SmartConnectors to the latest release.

For an overview of the SmartConnector installation and configuration process, see the SmartConnector User Guide. For complete installation instructions for a particular SmartConnector, see the configuration guide for that connector, available on the ArcSight Connectors Documentation page. The configuration guide provides specific device configuration information, installation parameters, and device event mappings to ESM fields.

ESM provides the ability to upgrade the SmartConnectors remotely using the `.aup` file. For detailed instructions about upgrading remotely, see the SmartConnector User Guide.

Publication Status

Released:

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 7.6.4)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!