Patch Release Notes
ArcSight™ ESM

Version 4.5 SP1, Patch 1
Build 4.5.1.5970.1

June 10, 2009

Patch Release Notes ArcSight™ ESM ,
Version 4.5 SP1, Patch 1

Revision History

Date	Product Version	Description
06/10/09	ArcSight™ ESM Version 4.5 SP1, Patch 1	Patch Release Notes for ArcSight™ ESM Version 4.5 SP1, Patch 1

ArcSight Customer Support

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

Contents

ArcSight ESM, Version 4.5 SP1, Patch 1

ESM Patch 4.5.1.5970.1

These release notes describe how to apply this patch release of ArcSight ESM. Instructions are included for each component, as well as other information about recent changes and open and closed issues.

This patch is for ArcSight ESM v4.5 SP1 only. If you are seeking to set up a fully current ESM v4.5 SP1 installation, refer to its own release notes for important additional information.

Purpose of this Patch

This patch focuses on addressing the Section 508 Federal accessibility mandate by addressing section 1194.22 Web-based intranet and internet information and applications for ArcSight Web Viewer.

Installing ESM Version 4.5 SP1 Patch 1

You can install this patch release using the platform-specific and component-specific executable files provided. Patch installers are available for all platforms.

Please keep the following points in mind when installing Patch 1.

- In some Solaris environments, when upgrading the ESM Manager and also when installing the solution packages, these actions do not complete. This could happen if your Solaris system does not meet the minimum system requirements. See the *ESM v4.5 SP1 Installation and Configuration Guide* for the minimum system requirements for a Solaris system.

- Make sure you execute `arcsight agentsetup -w` on the database component after installing and uninstalling the patch. Refer to the installation and uninstallation steps for the "ArcSight ESM Database" on page 2.

- **For all components and platforms:** Make sure that you have enough space (approximately three times the size of the patch installer) available *before* you begin to install the patch. If you run into disk space issues during installation, first create enough disk space, restore the component base build from the backup, then resume installation of the patch.

- Backup, patch install, and uninstall procedures require permissions for the relevant components. For example, to back up a database installation and install an Oracle critical patch update, you need database logon permissions. To back up the ArcSight Manager installation and install the Manager patch, you need Manager permissions. To install a patch, make sure that the user who owns the base build installation folder has full privileges on the PATH where the base build is installed.

- Due to issues related to configuration variability (AIX Tech Levels), a small number of users might experience issues with installation and uninstallation. It is a good practice to create a backup of the existing product before installation begins.

- Users who need to uninstall the software must be at the same user level as the original installer.

- For backup, patch install, and uninstall, we recommend that you log in to the target machine with a specific account name via telnet or SSH. If, instead, you switch accounts after logging in, then please be sure to specify the flag "**-**" for the **su** command, e.g., `su - <UserName>`

Platform-specific Information for Installing Patch 1

Each component has installation and rollback steps.

The patch installation instructions describe installation on all supported platforms. Platform-specific details are provided within the procedures below.

ArcSight ESM Database

This section provides step-by-step instructions on how to install and uninstall ESM v4.5 SP1, Patch 1 for ArcSight Database.

To Install

- Before you install the patch, make sure that the ArcSight Database's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.

- If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

1 Stop the Partition Archiver Agent.

Run:

`/etc/init.d/arc_oraclepartitionarchiver_db stop`

> `arc_oraclepartitionarchiver_db` is the default service name.

2 Back up the ArcSight Database directory by making a copy of it. Make sure to back up the database as the Oracle database owner. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.

> Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3 Download the executable file, `Patch-4.5.1.xxxx.1-DB-Solaris.bin,` from the ArcSight Software Download Site. (where `xxxx` stands for the build number.)

4 As the Oracle Database owner, run the following command:

`./Patch-4.5.1.xxxx.1-DB-Solaris.bin`

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

`./Patch-4.5.1.xxxx.1-DB-Solaris.bin -i console`

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing ArcSight Database's `ARCSIGHT_HOME` for your v4.5 SP1 database installation in the text box provided or navigate to the location by clicking **Choose…**

7 To restore the installer provided default location, click **Restore Default Folder**.

8 Click **Next**.

9 Choose a Link Location by clicking the appropriate radio button, then click **Next**.

10 Check the pre-installation summary to make sure that all the locations listed in it are correct and that you have enough disk space to install this patch.

11 Click **Install**.

12 Click **Done** on the Install Complete screen.

After installation of the database patch is complete **and** after you have installed the ArcSight Manager patch, update the Partition Archiver. These steps are required to upgrade the Partition Archiver version when viewed from the Console. Make sure that the Manager is running, then:

1 Run the following command from the Database `bin` directory to update the Partition Archiver:

`./arcsight agentsetup -w`

2   Click **Next** on the next few wizard screens until you see the screen that prompts you to either review or modify the parameters.

3   Select **I do not want to change any settings** and click **Next**.

4   Click **Finish** in the last screen.

Start the Partition Archiver Agent by running the following command:

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

> `arc_oraclepartitionarchiver_db` is the default service name.

To Uninstall

If needed, use the procedure below to roll back this patch installation.

> Before you begin to uninstall, make sure that the Database's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.

1   Stop the ArcSight Partition Archiver.

2   Run the uninstaller program as follows:

◆   From the directory where you created the links (your home folder or another location) when installing the database, run:

```
./Uninstall_ArcSight_Database_4.5_SP1Patch1
```

◆   Or, to uninstall in console mode, run

```
./Uninstall_ArcSight_Database_4.5_SP1Patch1 -i console
```

◆   If you did not create a link, execute the following command from the Database's `ARCSIGHT_HOME/UninstallerDataSP1Patch1:`

```
./Uninstall_ArcSight_DB_Patch
```

3   Click **Done** on the Uninstall Complete screen.

After uninstallation of the database patch is complete, update the Partition Archiver:

1   Uninstall the patch on the Manager.

2   Start the Manager.

3   Run the following command from the Database `bin` directory to update the Partition Archiver:

```
./arcsight agentsetup -w
```

4   Click **Next** on the wizard screens until you see the screen that prompts you to either review or modify the parameters.

5   Select **I do not want to change any settings** and click **Next**.

6   Click **Finish** in the last screen.

7   **On Windows Only**, click **Cancel** in the Archiver Service Configuration screen.

Start the Partition Archiver Agent by running the following command:

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

> `arc_oraclepartitionarchiver_db` is the default service name.

ArcSight ESM Manager

This section provides step-by-step instructions to install or uninstall the v4.5 SP1, Patch 1 for ArcSight Manager.

To Install

> - Before you install the patch, make sure that `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.
> - If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

1 Stop the ArcSight Manager.

2 Back up the Manager directory by making a copy. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.

> Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3 Download the executable file, `Patch-4.5.1.xxxx.1-Manager-Solaris.bin`, from the ArcSight Software Download Site. (where `xxxx` stands for the build number.)

4 While logged in as the ArcSight user, run the following command:

```
./Patch-4.5.1.xxxx.1-Manager-Solaris.bin
```

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

```
./Patch-4.5.1.xxxx.1-Manager-Solaris.bin -i console
```

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP1 Manager installation in the text box provided or navigate to the location by clicking **Choose…**

If you want to restore the installer provided default location, click **Restore Default Folder**.

7 Click **Next**.

8 Choose a Link Location by clicking the appropriate radio button, then click **Next**.

9 Check the pre-installation summary to make sure that all the locations listed are correct and that you have enough disk space to install this patch.

10 Click **Install**.

11 Click **Done** on the Install Complete screen.

To Uninstall

If needed, use the procedure below to roll back this patch installation.

> Before you begin to uninstall, make sure that the Manager's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.

1   Stop the ArcSight Manager.

2   Run the uninstaller program as follows:

  ◆ From the directory where you created the links when installing the Manager (your home folder or some other location), run:

    `./Uninstall_ArcSight_Manager_4.5_SP1Patch1`

  ◆ Or, to uninstall using console mode, run:

    `./Uninstall_ArcSight_Manager_4.5_SP1Patch1 -i console`

  ◆ If you did not create a link, execute the following command from the `ARCSIGHT_HOME\UninstallerDataSP1Patch1` directory:

    `./Uninstall_ArcSight_Manager_Patch`

3   Click **Done** on the Uninstall Complete screen.

ArcSight Console

This section provides step-by-step instructions on how to install or uninstall the v4.5 SP1, Patch 1 for ArcSight Console on Windows.

To Install

> • Before you install the patch, make sure that the Console's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.
>
> • If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

1   Exit the ArcSight Console.

2   Back up the Console directory by making a copy of it. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.

> ! Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3   Download the executable file, `Patch-4.5.1.xxxx.1-Console-Win.exe`, from the ArcSight Software Download Site. (where, `xxxx` stands for the build number.)

4   Double-click `Patch-4.5.1.xxxx.1-Console-Win.exe` to run it.

    The installer launches the Introduction window.

5   Read the instructions provided and click **Next**.

6   Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP1 Console installation in the text box provided or navigate to the location by clicking on **Choose...**

If you want to restore the installer provided default location, click **Restore Default Folder**.

7   Click **Next**.

8   Choose a Shortcut location by clicking the appropriate radio button and click **Next**.

9   Check the pre-installation summary to make sure that all the locations listed are correct and that you have enough disk space to install this patch.

10 Click **Install**.

11 Click **Done** on the Install Complete screen.

To Uninstall
If needed, use the procedure below to roll back this patch installation.

> Before you begin to uninstall, make sure that the Console's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.

1   Exit the ArcSight Console.

2   Run the uninstaller program as follows:

◆   Double-click the icon you created for the uninstaller when installing the Console. For example, if you created an uninstaller icon on your desktop, double-click that icon.

◆   If you created a link in the Start menu, click

Start->ArcSight Console SP1 Patch1-> Uninstall ArcSight Console 4.5 SP1 Patch 1

◆   Or, run the following from the Console's `ARCSIGHT_HOME\current\UninstallerDataSP1Patch1` directory:

`Uninstall_ArcSight_Console_Patch.exe`

3   Click **Done** on the Uninstall Complete screen.

ArcSight Web Server

This section provides step-by-step instructions on how to install or uninstall ESM v4.5 SP1, Patch 1 for ArcSight Web.

To Install

> • Before you install the patch, make sure that the Web's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.
>
> • If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

1 Stop the Web Server.

2 Backup the server directory (for example, `c:\arcsight\web`) by making a copy of it. Place the copy in a readily accessible location. This is just a precautionary measure so you can restore the original state, if necessary.

> Do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

3 Download the executable file, `Patch-4.5.1.xxxx.1-Web-Win.exe,` from the ArcSight Software Download Site. (where `xxxx` stands for the build number.)

4 While logged in as the ArcSight user, double-click `Patch-4.5.1.xxxx.1-Web-Win.exe` to run it.

The installer launches the Introduction window.

5 Read the instructions provided and click **Next**.

6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP1 ArcSight Web installation in the text box provided or navigate to the location by clicking **Choose…**

If you want to restore the installer provided default location, click **Restore Default Folder**.

7 Click **Next**.

8 Choose a Shortcut location by clicking the appropriate radio button, then click **Next**.

9 Check the pre-installation summary to make sure that all the locations listed in it are correct and that you have enough disk space to install this patch.

10 Click **Install**.

11 Click **Done** on the Install Complete screen.

To Uninstall

If needed, use the procedure to roll back this patch installation.

> Before you begin to uninstall, make sure that the Web's `ARCSIGHT_HOME` or any of its subdirectories are not being accessed by any open shells on your system.

1 Stop the ArcSight Web server.

  2   Run the uninstaller program as follows:

- Double-click the icon you created for the uninstaller when installing the ArcSight Web. For example, if you created an uninstaller icon on your desktop, double-click that icon.

- Or, if you created a link in the Start menu, click

  Start->ArcSight Web SP1 Patch1-> Uninstall ArcSight Web 4.5 SP1 Patch 1

- Or, run the following from the Web's `ARCSIGHT_HOME\UninstallerDataSP1Patch1` directory:

  `Uninstall_ArcSight_Web_Patch.exe`

  3   Click **Done** on the Uninstall Complete screen.

Open Issues in This Release

These open technical issues merit your review to avoid difficulties.

Install and Uninstall

Number	Description
35599 35786	When installing ArcSight Database, when prompted for directories for the `REDO` or `SYSTEM` volumes, if the directories you enter do not exist, you will not be able to proceed with the installation and will you will see an error. **Workaround**: Make sure that the directories for the `REDO` or `SYSTEM` volumes exist before installing the database. Create them if need be.
38367	When uninstalling a package, on very rare occasions, the **Uninstall Package** dialog does not display the package information correctly. **Workaround**: If you encounter this problem, exit the dialog and issue the uninstall command again.
39829	**Linux only:** While running the `runconsolesetup.sh` in the console mode, you will see an error message, "`chmod: cannot access '/arcsight/Console5199/current/config/console.properties' : No such file or directory`". Ignore this message and continue with the setup. The setup will not be affected.
42191	During ArcSight Web installation, when ArcSight Web attempts to connect to the Manager, if the Manager is not running, you will see an incorrect error message saying, "`Could not log in. The ArcSight Manager has a different version than your client.`" Workaround: Make sure that the Manager is running before you install ArcSight Web.
46153	**On Solaris:** For fresh ESM Manager installations/Manager upgrade, when the solutions packages get installed, occasionally the Manager installation/upgrade does not complete. **Workaround**: Please check the system requirements for your Solaris system in the "Supported Platforms" section of the "Installing ArcSight Manager" chapter in the *ESM Installation and Configuration Guide*, and make sure that your system meets the minimum requirement.

Number	Description
47129	**Windows only:** When installing or upgrading, the Partition Archiver wizard gives you information in the last screen of the wizard to install it as a service even if you chose to not install it as a service. Please ignore this information and continue with the installation/upgrade.
50562	While uninstalling the ArcSight Database component that was installed by an administrator/root, if a non-privileged user (oracle user) uninstalls it, the uninstall link/shortcut does not get deleted. **Workaround**: Delete the link manually.
51954, 52680, 52690, 54003	This release does not support spaces in install paths for the ArcSight Database, ESM Manager or ArcSight Web server. If there are spaces in the install paths, ESM Database, Manager, and ArcSight Web setup wizards might not work, and ESM Manager startup will generate exceptions. This is an issue on all platforms. **Workaround:** Please do not use spaces in ESM installation paths. The default install paths (e.g., C:/arcsight/Manager) do not include spaces. If you modify the install paths, just make sure there are no spaces in the directory names. Dashes (-) or underscores (_) can be used instead of spaces.
55853	The ArcSight Database installer does not include error checking or validation per Oracle supported schema user naming conventions. If the user names specified contain anything other than alphanumeric characters, the ArcSight Database installer will prevent create/recreate of the schema and display the following error code: `error ORA-00921: unexpected end of sql command` **Workaround**: For ArcSight Database install and schema setup, please keep in mind that Oracle supports only alphanumeric characters for database user names, and will not accept a dash (–) or underscore (_) in these names.
56750	**Solaris 64-bit platform**: Fresh install of ESM v4.5 SP1 in FIPS mode, or upgrade from v4.0 SP3 Patch 3 in FIPS mode to v4.5 SP 1 FIPS mode will fail. You will not be able to start the Manager after installation.

Upgrade

Number	Description
25121	If you used a custom logo for ArcSight Web, the logo may not show up correctly when you upgrade ArcSight Web. **Workaround**: Update the logo manually after you upgrade ArcSight Web. See the ArcSight Web *User's Guide* for details on how to do this.
47206	During upgrade to v4.5 SP1, the "SSL Client Only" authentication option gets selected by default. If you had set up your v4.0 SP3 Manager to use "Password Based and SSL Client Based Authentication" method, the authentication method selected in the upgrade wizard panel will still default to "SSL Client Only". **Workaround**: Make sure to change the authentication method back to "Password Based and SSL Client Based Authentication".

ArcSight ESM, Version 4.5 SP1, Patch 1

Number	Description
51319	For Oracle upgrades (e.g., from Oracle from 10.2.0.2 to 10.2.0.4), the Arcsight Database installer prompts you to specify the path to the directory where the previous ArcSight Database was installed (Previous ArcSight Software Directory). This might cause some confusion about whether users should specify the path to the ArcSight Database or to the Oracle Home directory. **Workaround:** The prompt to specify the path to the previous ArcSight Database software is not related to the location of the Oracle Home directory. This is simply asking for the path to the ArcSight Database software installation (e.g., C:\arcsight\db). If you don't have the previous arcsight database software directory available, enter the path of the current arcsight database software directory that you are installing to.
52394	File resources are not handled properly during ESM upgrades and this results in unassigned file resources after upgrade. For example, `.art` files are created as new file resources in ESM v4.5 SP1 and get new version IDs during the upgrade. The original files are stored in the Files resource under the Unassigned folder. **Workaround:** You can remove the unassigned `.art` files after an upgrade, since they are duplicates. The `.art` files can be safely deleted.
34527	The `arcdt` command cannot get session waits from the database. Launching the command to get session waits will generate an empty file. An example of such a command would be: `./arcsight arcdt session-waits -c 1 -f 10 -fmt html -sp -o /tmp/ss.html` This is caused by an issue with the JDBC driver.
42536	If you upgrade from any ESM version to an intermediate version, and then upgrade to the next newer version the same day (essentially, you are doing two incremental upgrades on the same day), the second upgrade will fail. **Workaround**: Wait till the execution of the next scheduled partition manager job which creates a new partition. You can let the Manager from the first upgrade run for a day (24 hours). This allows the Partition Manager to run more than once. It will create a new partition which allows the system to be recognized as upgraded to an intermediate version. Do the next upgrade after a day (24 hours).
48231	After upgrading to v4.5 SP1 ArcSight Database, if you try to manually archive some partitions that are within the online retention period and thus not eligible for archiving, those partitions will still get archived. **Workaround**: This issue will remain until the next scheduled maintenance takes place. Wait for the next scheduled partition archiver task to run. (The default time is 7:00pm.). That will resolve this issue.

Number	Description

54341, 54344	Upgrades from ESM v4.0 SP3 to ESM v.4.5 SP1 on systems that include Solutions packages may result in the following warnings during upgrade, or produce messages about invalid resources after upgrades (via a post-upgrade run of a "Resource Validation Report" or the **arcsight resvalidate** command).
	
	• Insider Threat Rule, Report, and Query: General Security – User Account Standard Violation
	
	    Workaround: You can remove these resources before or after the upgrade.
	
	• Insider Threat Asset: webproxy.kaxy.com
	
	    Workaround: Before or after upgrade, add the correct IP address for webproxy.kaxy.com
	
	• Any Solution Package: NRM – Quarantine rules
	
	    Workaround: Either choose a valid NRM connector in the rule action, or remove these rules if you are not using them. This can be done before or after upgrade.
	
	• PCI Dashboard: AntiVirus Activity Overview
	
	    Workaround: No workaround is necessary as the operation of the dashboard is not impacted
	
	If warnings related to these resources appear during the upgrade process, simply ignore these messages, or perform the suggested workarounds *before* upgrading.

55935	ESM Console upgrades from ESM v4.0 SP3 To ESM v4.5 SP1 do not properly read the security and login property settings (SSL files). If you run the upgrade and Console setup through to completion via the install wizard, you will still have to re-run Console setup. **Workaround**: Cancel the installation after the Console is installed, and run the ArcSight Console configuration wizard to configure property settings. In <ARCSIGHT_HOME>/<Console_Build>/current/bin, run the **arcsight consolesetup** at the command line. This way, SSL files are read and the Console can configure correctly.

ArcSight Database

Number	Description
53484	Certain reports run for several hours and then time out or fail with the error message: com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old This occurs because Oracle is using a sub-optimal query execution plan. In some cases, this can happen because of insufficient space in the ARC_TEMP table as well. **Workaround**: Set the report to query with a full scan database hint. For more information, refer to "Reports that query over a large time range with complex joins take a long time to run" section in Appendix B of the *ArcSight ESM Administrator's Guide*.
56718	The dbcheck utility fails to create a .zip file for its logs on Windows as indicated in the upgrade guide.

ArcSight Manager

Number	Description
17714	When a non-admin user runs a report, the report shows assets and cases even though a non-admin user does not have the rights to view the assets or cases.
33337	If the Send Logs utility detects that you do not have enough disk space to upload the logs, it displays an error that tells you to free up the disk space and retry log upload. **Workaround**: Exit the Send Logs utility and restart it after you have freed disk space on your machine.
36553	**Windows only:** The command line tools `arcsight managersvc start` and `arcsight managersvc stop` are not supported for this version of the product. **Workaround**: You can start or stop the Manager service from the Services window in the Control Panel. It is common to receive a "Service Timeout" the first time the Manager is started. This will not stop the Manager from starting properly.
37959	In hierarchical ESM deployments, when you add lower level Managers to the setup, make sure that you do not use the system tables that were exported from an existing lower level Manager. One of the system tables contains a unique Manager ID. This Manager ID is used by the upper level Manager to make certain decisions when reaching back for base events for forwarded correlation events. If you use the exported system tables for the new Manager, the Manager ID of the existing Manager from which you exported the tables gets copied to the newly added Manager thus having two Managers in the setup with the same Manager ID. When two lower level Managers have the same Manager ID, the higher level manager will pick a random lower level Manager, hence the results of the reach back could be unpredictable.
39988	When you have a large number of assets, it takes approximately 30 seconds to get a response after clicking the **Add** button in the Asset tab of the Zone editor to add an asset. **Workaround**: Instead of adding an asset in the Zone editor, we recommend that you right-click in the **Asset** channel on a specific Asset and select **Manual Zone** to do this.
40052	Moving assets from one group to another using the Move menu item does not work. **Workaround**: In the navigation pane, drag and drop the asset into the group that you want to move it into and select **Link** from the menu. Then delete the asset from the original group. For example, if you want to move an asset from group A to group B, drag the asset from group A and drop it into group B and select **Link** from the context menu. Then delete the asset from group A.
41193	On **Solaris**, in a High Availability environment, when you execute the `arcsight managerup` command, even if the Manager is running, you will see the following incorrect message: `No heartbeat response received.` Ignore this message as this will appear even though the Manager is running.

Number	Description
41582	Occasionally, when installing an exported package from a bundle file, you might receive the following error: `Install Failed: Resource in broker is newer than modified resource.` This error does not occur every time you attempt to install an exported package from a bundle. **Workaround**: Re-import the package.
42502	On a Manager with a large number of assets, for example 800,000 assets, selecting the **Stop** button in the Console when a recursive Asset channel is showing, and then restarting it will result in a communication error.
42730	You cannot move an asset using Auto Zone if the asset is locked.

43678	If the search index file becomes corrupted, the Search index will be out-of-date and you will see the following message in the Manager log:
	
	`[ERROR][default.com.arcsight.server.search.index.IndexRes ources][_init]`
	
	`java.io.IOException: read past EOF`
	
	Workaround: Regenerate the index by issuing the following command from the Manager `<ARCSIGHT_HOME>/bin` directory:
	
	`arcsight searchindex -a create`

47345	The index updater uses roughly the same amount of memory as the Java Heap Memory size, which could cause your system to potentially run out of memory. **Workaround**: Make sure to set your Manager's Java Heap Memory size to less than half of the physical RAM available on your system.
48529	You may not be able to create a report if it is based on Case Customization stage.
50794	In a hierarchical Manager setup, the base events for only some of the correlation events get forwarded to the upper level Manager, and this behavior is not predictable. If the upper level Manager needs the base events for these correlation events, and the base events are not present on the upper Manager, the base events get fetched on-demand when the user opens the correlation event in the event inspector panel on the upper level Manager.
51053	In some older versions of ESM, you may see some negative timestamp values in the server logs. You will see an error that begins with "`java.sql.SQLException: BC date found in...`" in the logs and the resources for which you see this error do not get loaded. **Workaround**: 1 Set the following property in the `<ARCSIGHT_HOME>/config/server.properties` file: `server.date.correction.recoverFromBCDate=true` 2 Restart the Manager. If you face this issue, please notify ArcSight Support about it, so that they can investigate its cause within your setup.

Number	Description
51112	Stages resources are editable from the ESM Console, although these should not be moved or customized. (See ESM Console Navigator > Stages resource tree.)
	Please keep stages provided as standard content in the given folders and do not move them into another folder. Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created. (For more information, See the topic "Standard Content" topic in the Console Help.)
51134	ESM integration commands launched from a chart view cannot pick up attribute values from the chart (as they can from grid views).
	For example, launching a URL integration command from a chart view in an active channel or query viewer results in a popup dialog asking for parameters values.
	This impacts ESM-TRM (Threat Response Manager) integration commands, as well as other third party integrations.
	Workaround: For this release, limit deployment of integration commands in the Console to chart views or inform Console users that they will need to manually type in parameter values when they run these commands from chart views.
53975	If you are not able to set up sending pager notifications through the pager service provider, please follow the workaround provided.
	Workaround: If your pager supports receiving e-mails, create notification destinations in ArcSight Console by providing the e-mail address of the pager in the e-mail destination.
54452	A `java.lang.InterruptedException` might be logged in the ESM Manager `server.std.out.logs` when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager.
	This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.
55969	**On Linux only**: The ESM Manager CPU utilization is higher than expected and impacts performance.
	The Manager's CPU utilization may become high especially in the kernel CPU utilization area. This issue may be specific to your system/hardware.
	Workaround: It may be possible to fix this issue by updating drivers or reinstalling the Linux operating system.
56061	When you integrate ESM with NSP 4.6, the NSP command **Generate Network Details as CEF Messages** does not generate CEF messages.
	When you integrate ESM with NSP 4.7, the NSP command **Generate Network Details as CEF Messages** works as expected.
56812	**On Red Hat Linux 5.3:** After you reboot the system, the Manager, Web, and Partition Archiver services do not start automatically.
	Workaround: Start the services manually. See the *ESM Installation and Configuration Guide* for details on how to do this.

ArcSight Console

Number	Description
24496	Drilldown from Event Graph data monitors to channels is not supported when the Event Graph data monitor uses Variables to retrieve or parse event information.
36748	After modifying an invalid resource, you must first save the changes by clicking the **Apply** button in the Editor panel before you validate the Resource. Since validation takes place on the Manager, the resource modifications must be uploaded and saved before they can be validated.
38270	While installing a package, if you cancel the installation before it is completed, the **Import** button will be disabled. **Workaround**: Refresh the Console or log in to the Console again to enable this button.
40627	In the standard field set for a channel, if you change the **Column Flip Limit** in the Preferences dialog even though you click **Apply** or **OK**, your change will not take effect. **Workaround**: Press the **Enter** key before you click **Apply** or **OK** in order for the new value to take effect.
41305	When a custom column in an active channel uses the "`$fieldname notation`" if the value of the field is null you will see the "`$fieldname`" value in the cell. This is a known issue.
42538	Performing unrelated UI operations in the Console after launching bulk asset operations (such as bulk Vulnerability assignments) can cause the operation to abort. **Workaround**: To avoid any possible problems, allow the bulk asset operation to complete before performing any further work in the Console UI.
42859	The report parameter dialog box that is brought up by right-clicking on an event in an Active Channel and selecting Report->Channel Report does not allow you to set the expiration time.
42972	In the Case channel, if you select a field set, the field set selector does not display the field set. This is a known issue.
43127	When editing a Case, if you right-click an event that has been assigned to the Case, the context menu will show an Event Graph operation item. This operation is not supported in the current release and choosing it will cause an error message to be displayed.
44028	**On Macintosh:** If you click **Help** menu and select **About** and then click on the **ArcSight Copyrights...** link in the About page, you will get a Java Exception. The exception is generated by an issue in the Grand-Rapid browser.
46426	When the Asset channel refreshes as new assets are added to it, some of the assets will not appear under the following scenarios: • If there are assets in the channel that are deleted and then re-added or updated. • One or more of the assets is selected and opened for edit in the edit window and the edit window has resized the asset channel viewer window.
49024	Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.

Number	Description
49608	In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range. **Workaround**: Delete the existing color mapping and create a new one with the color mapping of your choice.
50968	When you delete an escalation-level notification resource, you receive the error `Group does not exist` in the `console.log` file. This error is incorrect and can be ignored.
51072	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events return if variables are present in the Source Node Identifier.
51094	**On Unix systems**: The drag-and-drop feature does not work in the Console. **Workaround:** Use the cut-and-paste feature instead.
51245	**On Windows 64-bit platforms**, the ESM embedded browser does not properly support Secure Sockets Layer (SSL) or HTTPs. So, links from the ESM Console to secure sites result in pages that do not render properly in the embedded browser. The problems will manifest differently, depending on the content of the target Web page. For example, the initial page might display properly but buttons, links, or login mechanisms might not work properly. This impacts secure Knowledge Base articles, ESM-TRM (Threat Response Manager) integration commands, and any other third party integrations that use HTTPS URLs, since none of these will launch properly in the ESM embedded browser. **Workarounds:** • On Windows 64-bit platforms, use the external browser. To do this, choose Console menu option Edit > Preferences, click "Programs", and under "Preferred Web Browser" disable (uncheck) the option "Use the web browser embedded in ArcSight Console". Note that you can also specify a path to your preferred external browser here. Click Apply or OK to save these changes. With these new settings, integration commands, Knowledge Base, pages, etc. will launch in your preferred external Web browser, with support for HTTPS URLs. • Use Windows 32 bit platform and software, since HTTP URLs are supported on the embedded browser in Windows 32 bit versions of the ESM software. Note that you can install Windows 32-bit ESM software on Windows 64-bit systems.
51583	**On Macintosh only**: When you right-click in the Navigator on a resource, you will see an unexpected behavior where several of the menu choices might be already highlighted. This is a harmless issue, so you can continue by to clicking on the one you want to select.
52617	The Active Channel "Slide Show" feature (View > Slide Show > Start) maximizes the viewer to full screen and takes over the entire screen space. If you are working on multiple monitors, the slide show will take over your primary display. **Workaround:** If you have started the slide show from the Console, and want to exit out of it, press the Esc (Escape) key to stop it. This will return your Console to normal viewing mode and close the maximized channel windows. If possible, please avoid using this feature in this release.

Number	Description
53435	When you set the **Schedule Frequency** for a report, the **Next Run Time** field displays incorrectly in the Editor. Even though the time displays incorrectly, the report runs at the time specified in the editor.
53912	On the ESM Console, the Connector configuration settings do not support decimals for the "Limit event processing rate" option (Only integer settings are supported for this release), even though decimals are supported for this option on the Connector. **Note:** Select a Connector in the Navigator, right-click and choose "Configure" to bring up the configuration for that connector in the Inspector panel. Select the "Default" tab and then "Content" sub-tab. The "Limit event processing rate" option is under "Processing". Only integer settings are supported for this option via the Console.
54789	**On Linux platforms**: The ESM Console Help on the ESM embedded browser is not supported for this release. **Workaround:** Set Console preferences to launch Help in an external Web browser (instead of the default embedded browser). To do this, choose Edit > Preferences from the Console menus, click "Global Options", and enable (click to checkmark) "Launch Help in external web browser". If you want to change the Web browser used for the ESM Console, click "Programs", and provide the path for the External Browser you prefer to use. Click Apply or OK to save these changes. With these new settings, the Console Help will launch from all context Help menus in the Web browser of your choice, and display properly. More information about Help features and settings is provided in the Help topic "About the Online Help". **Note:** Starting the Web browser from the Console (for Help or Knowledge Base) might take a minute or more the first time the Web browser is used. Subsequent Web browser launches are much faster. If the system hosting the Console is rebooted, the first Web browser launch from the Console will be slow again.
56865	**On Linux only**: If you right-click on the port field in a channel and select Integration Commands->Portinfo (Linux) you will get an error.

ArcSight Web

Number	Description
24404	In ArcSight Web, channels with conditions that refer to an Event field that ends in `Resource` will fail. ArcSight Web does not support the use of these fields as a filter condition.
25667	If you create a Last State Data Monitor and add it to the dashboard in table and tile format, it will be rendered in tile format only when you view it in ArcSight Web. However, it renders correctly in the Console.
33318	Even though an ArcSight Webserver is connected to the Manager, it does not get listed in the Send Log wizard when it is run from the Manager to which the Webserver is connected. This feature is not supported for this release of the product.

Number	Description
39934	Viewing a Rule Verification channel in ArcSight Web is not supported in this release. **Workaround**: Use the Console to view this channel.
43254	Occasionally, when you drill down into the event details in a live channel, the details display for the event, but if you select another event and try to drill down to see its details, you will not be able to do so. **Workaround**: Restart ArcSight Web.
43327	ArcSight Web channels do not support sorting by a time field other than the one chosen as the channel time stamp. For example, a channel in ArcSight Web cannot use Manager Receipt Time as the timestamp and End Time as the sorting timestamp. Attempting to use such a channel in ArcSight Web will produce an error. **Workaround**: Use ArcSight Console to modify the channel sort column and then use it in ArcSight Web.
46969	When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an Active Channel. This is a known issue.
50878	If you use Internet Explorer browser, you will get an error when connecting to the server in FIPS mode. **Workaround**: When connecting to ArcSight Web in FIPS mode, make sure that you set Internet Explorer to use the TLS secure connection instead of SSL.
52336	On ArcSight Web, there is no row limit imposed on Query Viewer chart displays (unlike on the ESM Console). Query viewer charts with more than 100 rows do not display properly and are virtually unreadable. On the ESM Console, the chart renders only the first 100 rows and displays an error message indicating that only 100 rows can be properly displayed. No such restriction is available for query viewer charts on ArcSight Web dashboards, so some will not display properly on the Web. **Workaround:** ESM Administrators can set row limits on query viewers to control chart displays on both the Console and ArcSight Web. Determine which query viewers you want to display as charts. From the ESM Console, edit those query viewers to set the Row Limit to 100 (or less). To do this: 1 Log in to the ESM Console, choose **Query Viewers** in the Navigator, and right-click on the query viewer you want to edit. 2 On the Query Viewer Editor, click to disable (uncheck) **Use Default** (if it is enabled), then type in a row limit of 100 or less. 3 Click **Apply** or **OK** to save the changes.

Number	Description
55995	On Arcsight Web "Active Channels", the Event Inspector "Create Channel" feature does not create the channel filter properly.
	Clicking an event in an active channel brings up the Event Inspector, where you can view details on event fields or create a channel based on the value in an event field. Options are provided to (1) create a channel that filters only on the selected event field value or (2) add the selected event field value as a condition to the current channel filter. Option (1) does not work correctly, but instead simply adds the selected field value to the filter the same way option 2 does.
	Workaround: Manually modify the filter to specify the conditions you want. For example, to create a channel on an event field value for Priority, click an event in a channel to get the Event Inspector, click the Priority field and choose `Create Channel [Priority= <value>]` or `Create Channel [Priority != <value>]`. At this point, the filter conditions will not display correctly. Click "Modify", and edit the Condition Summary to remove the extra conditions and include only the values you want to filter for, e.g.: `Priority = "3"`. Now click ""Open" to view the modified channel or "Save Filter As…" to save it.
56005	If your session has expired and you click on a node in the Navigator tree to expand it, you will see a Java exception and ArcSight Web does not redirect you to the login page.
	Workaround: Start a new session.
56258	When you create a Case, if you set the Estimated Resource Time, it does not get set.
	Workaround: Define this setting on the Console. See the Console online help for steps to do this.

DST Issues

Number	Description
54713	If you had scheduled a report to run every two hours before the start of Daylight Saving Time and scheduled the first run to occur at an even numbered hour (for example 2:00 pm), once DST begins, the scheduled run for this report will occur on odd numbered hours (for example 1:00 am, 3:00 am, etc.). The interval will continue to be every 2 hours.
54749 55835	Depending on your time zone, you may see your scheduled tasks running off by 15 minutes to an hour. For example, scheduled tasks will run 15 minutes early in America/Guyana, whereas in Asia/Bahrain or Europe/London it will run one hour early, etc.
55230	When viewing reports you might encounter timestamps that are off by an hour.
	To convert the time in the database to your local time, the current time zone setting (including any DST offset) will be used. If the times you are querying are in a different DST setting, the local time reported will be off by one hour. For example, if you are in the Pacific timezone and in DST, and the time range you are querying is not in DST, the time will be off by one hour. For example, if it is June (in DST) and you query times in January (not in DST), your times will be corrected by the current timezone setting (in DST), even though the January times should not have DST applied to them

Analytics

28604	ArcSight ESM does not drop old Session List partitions automatically. Since the Session List entries are relatively small in number compared to events, this data usually does not need a lot of database space and need not be deleted.
31413	By default, reports with merged section column values will only print each value for the column once, vertically aligned in the center of the listing for that column value. **Workaround**: To improve readability when sections contain more than a page of data, we recommend that you set the vertical alignment of the relevant section column to top. This will cause the value of the section to appear at the top of the relevant section, thus making the report more readable.
34814	Certain queries against the asset database can perform poorly if written to include Variables that retrieve asset categories in an inefficient manner. **Workaround**: If you experience poor report performance in such a case, attempt to narrow the specification of the base asset category group beyond "`/All Asset Categories`" by using a deeper base asset category. For example, select "`/All Asset Categories/Site Asset Categories/Application`", rather than the top-level group. Expect a delay when running a report on 100,000 or more assets.
36051	When doing a search on resources, if your search criteria is an IP address using a wild card (such as 10.0.*) or a range of IP addresses, you may see an error. This error is likely due to the fact that the system has found too many entries matching your search criteria. **Workaround**: Refine your search criteria to be more specific and retry the search.
36148	To search for Resource IDs that begin with non-alphanumeric characters, (such as the Resource IDs for Trends and Queries) add double quotes around the ID. For example, to search for `^VVsOXg4BABCAIEuBhILMyg==` enter "`^VVsOXg4BABCAIEuBhILMyg==`" in the Query text field.
38832	When you display Assets in an Asset Channel, the Device Zone Network Name column does not get populated in the Grid view. **Workaround**: To view the details of an Asset, click the right-facing arrow in the first column to open the **Asset Detail** box.
39407	The Scheduled Time column in the Scheduled Runs view covers both time ranges for runs that have already occurred and for runs that are pending. As a result, you will see some discrepancy in the time ranges shown in the column. For example, against the runs that have already occurred you will see the lower end of the time range (For trends set to run hourly, if the time range is between 1:00 pm – 2:00 pm you will see 1:00 pm). The pending runs show the upper range (if the time range is between 1:00 pm – 2:00 pm you will see 2:00 pm). Trends that have already occurred will have a time difference that reflects the trend query schedule (e.g., one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (e.g., 24 hours if run once a day).

39932	Creating a new channel to verify rules results in the rule being applied correctly, but the generated events may not show up in the channel correctly because the correlated events don't match the filter. **Workaround**: Add an OR condition to the channel filter as "sessionID > 0" when you specify a filter for testing rules with replay.
40230	After editing the description for a trend, if another trend is dependent on it, the dependent trend will become invalid. **Workaround**: Disable the dependent trend in the trend editor and then re-enable it.
43456	If you create an asset, assign a category to it, and add the asset to a new package, when you uninstall the package, the category gets deleted too. **Workaround**: 1 Create a package and explicitly include the resources that should never be deleted in the package. 2 Export that package. If the resources under the parent groups change, then that package may need to be exported periodically.
43912	If you import the content of an older package into an existing newer package, the contents from the two packages get merged. The resulting package will consist of contents from both packages. The relationships will be merged, but the attributes will be picked up from the old package. **Workaround**: Export the new package to a bundle file so that you can recover it if need be. Then delete the new package before you import the old one.
50646	The column names of a generated report have a maximum width. If your column name exceeds that limit, the name is truncated and the truncated portion is replaced with a random alphanumeric character. For example, if you create a report that collects two minutes of data for two fields: **Original Agent Translated Zone External ID** and **Original Agent Translated Zone Resource**, the report displays the column names as **Original Agent translated Z** and **Original Agent Translated Z-0**. **Workaround**: Create a short alias for such columns in the report editor.

51280	Variables in some conditional statements in query definitions are improperly translated. Variables in GROUP BY and SELECT expressions are translated as CASE statements, and this causes problems in the GROUP BY part of the query definition. (The GROUP BY should be using the alias given to CASE statements in the SELECT statement, but this is not working properly.)
	Running a report or launching a Query Viewer with such a query generates an exception similar to this one:
	`The query run failed because of the following reason:`
	`com.arcsight.common.ArcSightException:` `com.arcsight.common.introspection.queryable.QueryableFetc` `hException:`
	`  Encountered persistence problem while fetching data:` `Unable to execute`
	`query: ORA-00979: not a GROUP BY expressionConditional` `variables in a SELECT statement with an aggregated field` `causes an Oracle exception (not a GROUP BY expression)`
	Workaround: Remove all the variable fields from the Select clause in the query, then add them back one at a time, updating and running the report after adding each variable. This allows you to know which variable does not translate properly, giving you the option to modify or replace that variable. Refer to the Console online help for instructions on how to do this.
54507	Verify Rules with Events (replay with rules) does not work for these types of active lists:
	• an event-based active list with values
	• a field-based active list with values, where all fields are mapped to event fields
	Verify Rules with Events does work for other types of active lists. Also, valid active lists work properly with real-time rules when they are deployed, including the two types of active lists described above.
55314	Variable names that contain dashes or hyphens (-) in the name do not work properly when included on the right side of a comparison in a condition statement.
	For example, consider a Rule with a condition that compares the JME argument `sqrt(4)` to a variable named `abc-cde`, where the value of `abc-cde` is: `add (2.0,3.0)`.
	This rule will not trigger successfully, and the logs will show an exception indicating ESM is "unable to evaluate rule".
	Workaround: Please do not use dashes or hyphens (-) in variable names as a best practice to avoid this problem altogether. Underscores (_) are acceptable in variable names, but upper and lower case letters only are best.
56345	If your query uses the getSessionData variable to join a session list with an active list you will get an error when you try to run the report or view the channel.

Connectors

Number	Description
45785	The Asset Import SmartConnector ignores the category content in the second CSV entry (with the same IP address) if a duplicate asset is imported. **Workaround:** To avoid creating a duplicate asset for the imported asset, complete all required category URLs in a single CSV entry.

46902	Running `arcsight agent sendlogs` command from the Connector's `<ARCSIGHT_HOME>` when the Connector is installed in FIPS mode results in the following error:
	
	`Exception in thread "main" java.lang.NullPointerException`
	`at java.util.Hashtable.put(Hashtable.java:394)`
	`at java.util.Properties.setProperty(Properties.java:143)`
	`at java.lang.System.setProperty(System.java:731)`
	`atcom.arcsight.install.wizard.WizardProcessorBase.run(WizardProcessorBa`
	`se.java:118)`
	`atcom.arcsight.install.wizard.WizardProcessorBase.run(WizardProcessorBa`
	`se.java:89)`
	`atcom.arcsight.tools.logsender.LogSenderWizard.main(LogSenderWizard.jav`
	`a:2301)`
	
	`Exiting...`
	
	Workaround:
	
	You can use the sendlogs feature by clicking on **Tools->Sendlogs** in the Console.

46940	While installing a Connector in default mode, if you use a Demo certificate to connect to a Manager running in default mode, you will get an error saying "Manager Certificate not trusted. Please check your SSL configuration." **Workaround:** While installing the Connector: 1 When you get to the wizard screen that prompts you to select the destination type that you want to configure for the SmartConnector, **do not** click Next and leave the wizard running. 2 Open a shell/command prompt window. 3 Run the following command from `<ARCSIGHT_HOME>/current/bin` directory: `arcsight connector tempca -ac` 4 Go back to the wizard and complete the installation.
47377	If a Connector tries to reconnect to the Manager after an earlier attempt to connect timed out, the Connector sends batches in CSV format instead of binary format. This generates multiple `agent_error_batch*<AgentID>.bin` files under the Manager's `logs/default` directory. Ignore these files as they do not cause any data loss.

Localization

This release does not support localized environments. This section provides information on related open issues.

Number	Description
45090	A field (Data Monitor Type) in the Attribute tab of Data Monitor Editor is only partially displayed. **Workaround:** Expand the **Inspect/Edit** pane until you see the full text in the Data Monitor Type field.
45278	On **Solaris**, when you generate a report in the PDF format, the contents of the report appear to be garbled. **Workaround**: Generate the report in a format other than PDF.
46242	When editing a Channel in ArcSight Web, if you use MatchesFilter option and add a filter using the & operator, the resulting query displays some random characters and the page freezes.
48266	The French version of the Console may display double quotes instead of single quotes when displaying l′ or d′ (for example, l" or d" instead of l' or d')
50213	In localized versions of ESM, when generating a report in PDF format, the characters within the report appear garbled. This is due to a problem with a 3rd party reporting package used. **Workaround**: Use other formats such as HTML, CSV, etc. to generate reports.
55823	In Traditional Chinese and Japanese environments: Assigning a hotkey to a resource is not supported for this release.