# Release Notes
# ArcSight™ ESM

Version 4.5 SP1

Build 4.5.1.5926.0

June 4, 2009

## Release Notes ArcSight™ ESM, Version 4.5 SP1

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

This document is ArcSight Confidential.

Revision History

| Date | Product Version | Description |
|---|---|---|
| 06/04/09 | ArcSight™ ESM Version 4.5 SP1 | Added information about hotfix number 57485 in the usage notes section "Incorrect Console Title bar License Description" |
| 04/20/09 | ArcSight™ ESM Version 4.5 SP1 | Documents ESM-related information for v4.5 SP1 |

### ArcSight Customer Support

| | |
|---|---|
| **Phone** | 1-866-535-3285 (North America)<br>+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

## Welcome to ArcSight ESM v4.5 SP1

ArcSight Enterprise Security Management (ESM) v4.5 SP1 introduces a new feature set that broadens its security information and event management functionality. This functionality includes query viewers for analysis, network modeling wizards, use cases for content deployment and an improved third party integrations through integrations commands. ArcSight ESM v4.5 SP1 also includes new correlation enhancements such as new variables, CCE field comparisons, data monitor enhancements and filter debugging capabilities.

ESM provides the ability to monitor and model your network and user behavior, quickly customizing the product to your needs so you can leverage its core technology to solve IT security challenges such as external threat management, regulatory compliance, insider threat prevention, and other scenarios.

Refer to the *ESM Reviewer's Guide* for the details on the new features.

## What's Introduced in this Release?

This release introduces a new feature set as outlined below:

- **Query Viewers**

  ArcSight ESM v4.5 SP1 introduces the Query Viewer, a new resource for defining and running SQL queries to provide a high level summary that can be used to monitor system health, and reveal trends. It also allows for drill-down investigation on various ESM data sources, for example, trends, lists, assets, events, etc.

- **Network Modeling Wizard**

  This release of ESM includes a network modeling wizard which enables you to quickly populate the ESM network model by batch loading asset and zone information into the ESM Manager from a pre-populated Comma Separated Values (CSV) files.

- **Use Cases**

  ArcSight ESM v4.5 SP1 introduces use cases, a resource collection that addresses common security issues and business requirements. Use cases are installed with a wizard which automates configuration of the resources involved in the use case. The wizard steps through questions on event sources to use, data sets to populate active lists, reports preferences, notifications, etc. then configures the use case accordingly.

- **Integration Commands**

  Starting with ESM v4.5 SP1, the Console offers an improved application integration capability to configure and launch commands, tools, and views in other applications, including other ArcSight products through the Integration Commands resource. Integration Commands provide a centralized location for configuring custom scripts, URLs, and CounterACT SmartConnector commands, and integrate them into the Console UI in various contexts.

# Enhancements in ESM v4.5 SP1

There have been several enhancements made to existing ESM features. The ArcSight ESM system enhancements include enhancements in the areas of Correlation, Variables, Rules, Data Monitor, Filter debugging, improved resource auditing, and Console.

## Correlation Enhancements

- Condition Editing Enhancements

  The Common Condition Editor (CCE) has been enhanced to provide the ability to define inner/within-event field comparisons as part of rule conditions.

- Pattern Discovery Enhancements

  Pattern Discovery has been enhanced to offer the ability to add results to an active or session list action, and improve system performance when analyzing event patterns.

- Variable Enhancements

  Variables functions have been enhanced to include: new and enhanced String Functions LastIndexOf and Evaluate Velocity Template, new Type Conversion Functions: ConvertListToString and GetSizeOfList, and better support for Java Mathematical Expression. Please see the ESM Help and *ESM User's Guide* for full details on all supported functions for Variables.

- Data Monitor Enhancements

  ArcSight ESM v4.5 SP1 enhances Data Monitors (DM) by improving their offering in the following areas:

  - Hierarchy Map Data Monitor has been enhanced to offer a redefined group fields view, more drill-down options, and enhanced visualization tools for controlling the map displays.
  - Data monitors now offer the ability to preserve their state after unexpected restart.
  - Top Value Count Data Monitors now offer the ability to generate correlation events.

- Filter Debugging

  ESM v4.5 SP1 introduces a filter debugging option within the active channel that enables you to compare the conditions in a selected filter, match with the metadata that describes the selected event to determine whether there are any mismatches, and identify which filter conditions are not matching the event details.

## Improved Resource Auditing

Updates to existing resources are logged as audit events. See “Resources (Configuration Events Common to All Resources)” in the *ESM User's Guide* or the Console Help for a detailed description.

If you would like to get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property on the ESM Manager to specify which resources should show extended audit event information. See the “Extending Audit Event Logging” section in the “Managing Resources” chapter of *ESM Administrator's Guide* for more details.

## Console Enhancements

The following enhancements have been made to the ArcSight Console:

- User Permission Enhancements

  As part of ESM v4.5 SP1, the Access Control List (ACLs) editor has been redesigned to provide a more user-friendly interface and offers a new option to define who has permissions to deploy data monitors.

- Short Cut Enhancements

  You now have the ability to define and manage customized keyboard shortcuts for common actions performed locally in the console.

- Asset Location Enhancements

  You can now personalize the format used for defining the latitude and longitude used for Asset Location description.

### ArcSight Content Enhancements

The ArcSight Administration Foundation package has been restructured and updated to provide statistics about the health and performance of ArcSight ESM and its components, such as ArcSight Manager, ArcSight Database, and ArcSight Connectors.

## New Platform Coverage

Please review the *ArcSight ESM v4.5 SP1 Platform Product Lifecycle* document for details on OS platform support for the Manager, Database, Console, and ArcSight Web components. Here are some highlights concerning newly added platform support:

- **ESM v4.5 SP1 64-bit Support**

  As part of ESM v4.5 SP1 a 64-bit JVM installer is available for ArcSight Manager for all of the 64-bit platforms supported.

- **Red Hat Enterprise Linux 5.3 (RHEL 5) AS**

  ArcSight ESM v4.5 SP1 Manager, Database and ArcSight Web support is offered for Red Hat Enterprise Linux 5.3 (RHEL 5) AS.

- **Microsoft Windows Server 2008 R2**

  ArcSight ESM v4.5 SP1 Manager and ArcSight Web support is offered for Microsoft Windows Server 2008.

- **JRE Support**

  ESM v4.5 SP1 provides support for JRE 1.6, update 11.

## Upgrade Support for this Release

Upgrade in this release is supported from ESM v4.0 SP3 to v4.5 SP1. Please refer to the upgrade guide for more information on upgrade instructions.

## Installation and Configuration

For installation instructions, refer to the *ArcSight ESM Installation and Configuration Guide*.

## Forwarding Connector

The ArcSight Forwarding Connector (formerly the ArcSight Manager SmartConnector) lets you receive events from a source ESM Manager installation and send them to a secondary/destination ESM Manager, a non-ESM location, or to an ArcSight Logger.

- The non FIPS compliant Forwarding Connector supported by ESM v4.5 SP1 is ArcSight-4.7.1.5260.0-SuperConnector.
- The FIPS compliant Forwarding Connector supported by ESM v4.0 SP3 is ArcSight-4.0.8.5012.0-SuperConnector.

Please refer to the *SmartConnector Configuration Guide for ArcSight Forwarding Connector* for more information.

# Usage Notes

Please review the following points to ensure smooth operation.

## Incorrect Console Title Bar License Description

When you install or upgrade to ESM v4.5 SP1 using a license key generated before May 2009, you will see an incorrect description for the license in the title bar of the Console. The Console title bar displays 'Internal license, used for development and QA'.

To correct the title, install the 4.5.1.0.57485 hotfix which is available on the ArcSight Customer Support site (https://support.arcsight.com/).

## Adobe Flash Player Limitation

Due to a limitation in Adobe Flash Player, to view dashboards within ArcSight Web on a 64-bit operating system, you are required to use a 32-bit browser with a 32-bit version of Flash player installed. Refer to the Adobe web site that discusses this issue (http://www.adobe.com/go/6b3af6c9).

## Case Customization

The data type used for case stage has been updated to be of enumeration data type instead of the String data type used in previous ESM releases. So, if you had Case queries in your system that used string operators on the Case Stage field (for example "stage startsWith 'F'"), you will be required to manually fix those conditions to use operators valid on enumeration data types. For example, if you have a condition "stage startsWith 'F'" and there are two possible enumeration values (2, Final) and (5, Follow-up), you should change the condition to "stage = Final or stage = Follow-up".

Please also see bug "51112" on page 19 for other notes on this topic.

## Change in Report Output for CSV format

The information in this section is applicable only if you are upgrading from ESM v3.x to v4.5 SP1.

ESM v4.5 SP1 does not support plotting the chart component for reports generated in the CSV format. But, adding this property in the `server.properties` file:

```
report.csv.header=true
```

will add reportName, startTime, endTime, and timeZone information in the CSV report.

If you need a chart, you can generate the report in PDF format.

Starting in ESM v4.0, generating reports in CSV format is no longer supported.

## Oracle’s Dynamic Sampling and Query Performance

Dynamic sampling levels in Oracle determine how Oracle would do data sampling at query execution time to derive an optimal execution plan.

Starting in ESM v4.5 SP1, Active Channel queries use dynamic sampling level 2 instead of level 4. (Level 4 was the default in ESM v4.0 SP3.) The level has been changed because of a bug in Oracle optimizer that sometimes causes the time spent in sampling to be very high, slowing down the overall channel.

For reports, trends, or any other queries, the dynamic sampling level continues to be at level 4.

If you observe any query performance issues, refer to the *ArcSight ESM Administrator’s Guide* topic on “Query and Trend Performance Tuning” (under “Troubleshooting). Try those troubleshooting recommendations about regenerating event statistics, and so forth. If the performance issue still does not get resolved, contact ArcSight Customer Support for help in addressing these issues.

## Logging in as systemuser while using Active Directory or LDAP

To login as systemuser while using Active Directory or LDAP, you have to map the ESM user with the Active Directory or LDAP user. To do so:

1. To enable ArcSight systemuser run the following from the Manager’s `bin` directory:

   ```
   arcsight configsystemuser
   ```

2. When prompted, set the External ID and password for the systemuser.

   **Important**:

   - The External ID must be identical to the user ID set for your Active Directory/LDAP account.
   - The External ID should not contain a space.

3. Log into the Console with username `systemuser` and the password set in the above step.

4. Stop the Manager by running the following from the Manager’s bin directory:

   ```
   arcsight managerstop
   ```

5. Restart the Manager by running the following from the Manager’s `bin` directory:

   ```
   arcsight manager
   ```

6. Start the Console and log in with username `systemuser` and your password which is linked to the Active Directory/LDAP account.

## Miscellaneous Notes

Please take into account the following usage notes:

1. New installations of the localized version of ESM have not been certified but are supported. Upgrades will be supported in a follow on release. “Localization” on page 29 provides information on localization-related open issues.

2 FIPS mode is supported but not certified for this release. Please see TTP "56750" on page 14 for details on an issue with installing in FIPS mode on the Solaris 64-bit platform.

# Geographical Information Update

ArcSight Express contains recent geographical information used in graphic displays. The version is GeoIP-532_20090201.

# Vulnerability Updates

This release of ArcSight Express includes recent vulnerability mappings (February 2009 Context Update).

| Device | Vulnerability Updates |
|---|---|
| McAfee HIPS 7.0 | Updated CVE, MSSB |
| Radware DefensePro | Updated CVE, MSSB |
| Cisco Secure IDS S376 | Updated Bugtraq, CVE |
| FunkWerk (VarySys Technologies) PacketAlarm | Updated Bugtraq, CVE, Nessus, Arachnids, MSSB |
| Juniper/Netscreen IDP update 1349 | Updated Bugtraq, CVE, MSSB, X-Force, CERT, MSKB |
| McAfee Intrushield | Updated CVE, MSSB |
| TippingPoint UnityOne DV7626 | Updated CVE, Bugtraq, MSSB |
| Snort / Sourcefire SEU 189 | Updated Bugtraq, MSSB, CVE |
| Fortigate Fortinet | Bugtraq, CVE, MSSB, X-Force |
| ISS SiteProtector | Updated X-Force, CVE, CERT, Bugtraq, MSSB |

# Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM has been certified with the Oracle critical patch update (CPU) for April, 2009. Certification has been established on all supported platforms with Oracle 10.2.0.4. Please visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

| Platform | CPU April 2009 Patch |
|---|---|
| Windows 32 | p8307237_10204_Win32.zip |
| Windows 64 (AMD64-EM64T) | p8307238_10204_MSWIN-x86-64.zip |
| Linux 32 | p8290506_10204_Linux-x86.zip |
| Linux x86-64 | p8290506_10204_Linux-x86-64.zip |
| AIX | p8290506_10204_AIX5L.zip |
| Solaris 64 | p8290506_10204_Solaris-64.zip |

# OPatch

Please visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment..

| Platform | OPatch April 2009 |
|---|---|
| Linux 32 | p6880880_102000_LINUX.zip |
| Linux x86-64 | p6880880_102000_Linux-x86-64.zip |
| Solaris 64 | p6880880_102000_SOLARIS64.zip |
| Windows 64 (AMD64-EM64T) | p6880880_102000_MSWIN-x86-64.zip |
| Windows 32 | p6880880_102000_WINNT.zip |
| AIX | p6880880_102000_AIX64-5L.zip |

# To Apply the CPU

1. From the Product Download section of the ArcSight Customer Support site (https://support.arcsight.com/), download both the Oracle CPU and OPatch as follows:
   - Download the correct Oracle CPU package for your platform (see the tables above) and unzip it under your working directory.
   - Download the Oracle 10g OPatch file for your platform.
2. Install the OPatch as follows:
   - Review the README file in the OPatch zip archive.
   - Extract the contents of the OPatch zip file under $ORACLE_HOME.
3. Stop the ArcSight Manager and Partition Archiver, and also stop the Oracle instance, and TNS listener.
4. Set the OPatch binary in PATH.
5. Read the next section in this document, "WorkArounds for Known Issues in Oracle CPU" on page 8.
6. Install the CPU (that you downloaded in Step 1) according to the steps outlined in the README in the CPU zip package for your platform.
7. Replace references to "OPatch" in the commands with `$ARCSIGHT_HOME/bin/arcdbutil patch`.

   For example,

   **On Windows:**

   If the README says:

   ```
   >opatch apply
   ```

   Then use the following command instead:

   ```
   $ARCSIGHT_HOME\bin\arcdbutil patch apply
   ```

   **On Unix:**

   If the README says:

```
>opatch napply -skip_subset -skip_duplicate
```

Then use the following command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch napply -skip_subset
-skip_duplicate
```

More information about Oracle-specific steps is provided in the README that accompanies the Oracle CPU. Be sure to review the README carefully and follow those instructions.

8 To complete the installation, follow the “Post Installation Instructions...” steps in the `README`.

9 Restart the database and the TNS Listener.

10 Restart the Partition Archiver and the ArcSight Manager.

# WorkArounds for Known Issues in Oracle CPU

The following subsections provide you with workarounds for issues related to Oracle CPU on the different platforms.

## With Windows for Oracle 10g

In some cases, the CPU application can fail with the following error:

```
OUI-67124:Copy failed from "<source>" to "<destination>"

OPatch failed with error code 115
```

This happens because there are other processes running that locked the file in question. These processes that caused the lock might be related to Oracle or not. To work around this, reboot the machine and retry the patch application steps again.

## With 32-bit Linux Using a Large Instance

If your ArcSight Database is running on a 32-bit Linux machine with the SMP kernel and your system is configured to use memory between 2 GB and 4 GB (the default configuration of the Large template), then perform the following steps after applying an Oracle Patch or an Oracle Patch Set (for example, a Critical Patch Update or the patch set for 10.2.0.4) to your ArcSight Database:

1 Log into the database machine as Oracle software owner (by default, Oracle).

2 Shut down the Oracle database, the TNS listener, and all other Oracle services (if any).

3 Run these commands:

```
cd $ORACLE_HOME/rdbms/lib

mv ksms.s ksms.s.org; mv ksms.o ksms.o.org

$ORACLE_HOME/bin/genksms -s 0x15000000 > ksms.s

make -f ins_rdbms.mk ksms.o

make -f ins_rdbms.mk ioracle
```

4 Restart the database server and the TNS listener.

This enables the ArcSight database to utilize the extended memory. Oracle cannot restart if this procedure is not followed. If the above commands display errors, call ArcSight Customer Support. If you are using your own Oracle software license, contact Oracle.

# Issues Fixed in this Release

## Installation and Upgrade

| Number | Description |
|---|---|
| 44711 | If you had moved/deleted the default system asset group, then recreated it, the IDs and URIs got out of synchronization. As a result, when you tried to upgrade the Manager, the upgrade would fail. This group is now locked and can no longer be deleted. |
| 53329 | During upgrade, the **Java Heap Memory Size** panel in the ArcSight Manager Configuration Wizard displayed the default heap size instead of the java heap memory size selected during a previous configuration. The Java Heap Memory Size now gets transferred during upgrade. |

## Database

| Number | Description |
|---|---|
| 31009 | Fixed an issue where partition names did not match the time range of the data within the partition. This happened for certain timezones only. |

## Manager

| Number | Description |
|---|---|
| 32997 | Zones & dark address space mappings are now up-to-date in ESM. |
| 43426 | Fixed an issue where if the Manager and Console were in different time zones, the Sendlogs utility did not take that into account. It collected logs from the Manager without considering that it had a different time zone as a result the timestamp in the logs were incorrect. |
| 52951, 52504 | Fixed an issue where the ArcSight Manager would encounter an “Out of Memory” exception while running Pattern Discovery. |
| 52615, 47432 | Fixed issues causing out-of-memory conditions on 64-bit systems. Increased the permanent generation memory pool in the Java Virtual Machine (JVM) that ships with ESM to 192 M. This is a setting in `server.defaults.wrapper.conf` file. |
| 53355 | Fixed an out-of-memory error where ESM would terminate when the database transaction was rolled back. |

## ArcSight Console

| Number | Description |
|---|---|
| 21929 | Fixed an issue where the change to an existing DV was not reflected in the Channel immediately. You had to restart the channel for the change to take effect. You do not need to restart the channel any more. |
| 35285 | Some information messages that appear as a result of rule actions, were displayed in a modal dialog. Every time the dialogs popped up it would distract the user. The messages do not appear in a modal dialog any more. |
| 35816 | Fixed an issue in the reports that used stack chart labels, where the titles for the x and y axis were illegible. |
| 38737 | Within a Data Monitor, if you tried to sort a column the column to its right would get sorted instead of the column you wanted to sort. Also, you were unable to sort the right most column. These issues have now been fixed. |
| 42202 | If you made a change to an inline filter in an Active Channel, the field set information got removed from the Active Channel. This issue has now been fixed. |
| 43601 | If you ran a report that is based on the query which is based on the trend which you did not have access to, the Console would freeze without showing any errors and no exceptions were logged into the `console.log` file. This issue is now fixed. |
| 44126 | If you created a field set for a case used on a channel it did not get saved with that channel. You had to reapply that field set every time you opened the channel. This issue is now fixed. |
| 44300 | In the SetEventField text box if you entered a value containing either a backslash, comma, or double quotes, the velocity strings got mangled.<br>**Workaround**: This problem can be avoided by following these rules:<br>• If an input contains commas, the input is interpreted as a list of values. Add double quotes around your input if this is not what you want.<br>• "\" should be always be escaped by adding another "\" to make "\\".<br>• Double quote character in the middle of the input should always be escaped by adding "\" before it.<br>• If the input is a list of values such as abc, 123, efg, parenthesis are added automatically around the input to form (abc,123,efg) |

| Number | Description |
|---|---|
| 46090 | In the current release, the Network Configuration Manager (NCM) network device user rights group is an “admin” user group by default, and this causes some confusion about access control lists (ACLs) management. To view network devices and manage ACLs, a user must be a member of an admin User group with rights to view routers, switches, etc.<br>For more information on managing user and user group permissions and ACLs, please see the ESM Console Help topic: Managing Resources (for Administrators) > Managing Permissions and Resources.<br>As a follow-on issue, a feature request has been logged to move the NCM group out of the admin user group and into its own separate group. |
| 45562 | Fixed an issue with Hierarchy Map Data Monitor where a right-click “Show Events” choice on a tree map block resulted in opening a channel with no events displayed. The channel showed a message “No data matched this query”. The problem was caused by an invalid filter on the channel that included a “/” in front of the event name. If you manually removed the “/” from the filter, the channel would populate properly.<br>In this release, this issue is fixed; a right-click “Show Events” choice on a Hierarchy Map block will bring up a channel populated with the relevant events based on a valid filter. |
| 47750 | An issue where entries from a fields-based active list did not populate a Last State Data Monitor was not reproducible. |
| 51067 | On Windows Vista (64- and 32-bit): ArcSight recommended that you don’t install ArcSight Console in the Program Files directory. If you installed the Console in the Program Files directory as user *arcsight*, the `console.log` and `velocity.log` files did not get created in the logs directory on the Console. |
| 51487, 47390 | Fixed an issue on the ESM Console Common Conditions Editor (CCE) UI with `InSubnet` and `NOT InSubnet` condition statements. These conditions were not working properly in previous releases (for example, condition statements containing `InSubnet` would re-set to the same subnet range when you clicked “Apply” on the CCE Editor). Both the `InSubnet` conditional statement and its negation are working now. |
| 52098 | When you connected to the ArcSight Manager, you encountered an error specifying that the Manager license was not valid if the Manager certificate was not found.<br>This will not happen in this release, because you will be prompted to accept the Manager’s certificate. |
| 53414 | Fixed an issue on Windows Vista (64-bit) where ArcSight Console froze if a non-admin user tried to export a resource package to certain folders. |

## ArcSight Web

| Number | Description |
|---|---|
| 53960 | If you modified the **Use as Timestamp** field on a channel, you received an error and the modification was not made. This issue has now been fixed. |

| Number | Description |
|---|---|
| 53961 | Filter conditions were lost when you changed a channel parameter.<br>This occurred only in ArcSight Web if you provided an invalid parameter value and received an error. The next time you changed the parameter to a valid value and then opened the channel, the filter conditions were lost. This issue has been fixed in this release. |

## Analytics

| Number | Description |
|---|---|
| 13476 | When creating a report, if you chose two or more<br>users to receive e-mail notifications, the report got created but neither user received the notification e-mail.<br>This issue has been fixed such that both users receive e-mail notifications now. |
| 27469 | When executing a Report ad hoc using the **Run** button in the editor pane or also selecting Run from the context menu, you received an error:<br>`[10:14:58] Report creation failed: Error while executing command: Server returned HTTP response code: 502 for URL: https://semweb.swissptt:443/arcsight/servlet/XmlRpc` |
| 32981 | Fixed an issue which caused the Brute Force Login Rules to not account for Target User IDs, and the rule actions to not set the categorization of the correlation event properly. |
| 45475 | When a Connector went down, content monitoring was done based on Moving Average Data Monitors which was not a reliable way of monitoring it.<br>Enhancements have been made to the way Connectors and devices get monitored by basing the content on internal events generated by the Manager and the Connectors both of which generate an event when a Connector is down or when the Connector heartbeat times out. |
| 49075 | Fixed an issue where disabled rules were included in rule validation. Disabled rules are no longer included in rule validation and, therefore, will not result in error messages even if they are invalid.<br>On a related note, Insider Threat Solution packages were generating run-time errors because of a rule with an incorrect regular expression: `java.util.regex.PatternSyntaxException: Illegal repetition near index 14 ^\W*\.\W{1}\.\W{*}$`<br>The errors would still display even after the related rule was automatically disabled.<br>The Insider Threat Solution package content has since been corrected for this error. |
| 50298, 50258 | Fixed an issue in which reports formatted as CSV files did not display report parameters. A report formatted in PDF would show the parameters (e.g,. Start Time, End Time, and Manager Time Zone) as labels for columns or rows, whereas a CSV report on the same data would show only the data, but not the parameter-based labels.<br>CSV formatted reports now show the parameter-based labels for the data, just like the PDF-style reports. |

| Number | Description |
|---|---|
| 50442 | Fixed an issue where Swedish characters were not recognized by ESM, even with UTF-8 characters. Previous to this release, rules with condition statements labeled with Swedish names (e.g., ÅÄÖ) would show up as invalid and produce error messages similar to this one:<br>`1,com.arcsight.server.rules.resource.a: com.arcsight.rulesengine.opsj.OPSJRulesBuilderException: com.arcsight.rulesengine.f: [Translating: C:\\arcsight\\Manager1\\rules\\Temp\\System_Comp.opsj] C:\\arcsight\\Manager1\\rules\\Temp\\System_Comp.opsj:23: syntax error \nactual: char """ expecting: char "*"\C char "-"\C INTCONST\C LONGCONST\C FLOATCONST\C DOUBLECONST\C STRINGCONST\C CHARCONST\C FALSE\C TRUE\C NULL\C THISITEM\C THISOBJECT\C IDENT C:\\arcsight\\Manager1\\rules\\Temp\\System_Comp.opsj:23: end-of-line in string literal`<br>Swedish characters are now supported in ESM on databases with standard English and UTF-8 character sets. |
| 51461 | An issue where the Asset Import Connector failed to recognize the re-naming of an imported asset to something other than the default (via the `scanner-event.auto-create.asset.name.template` setting in `server.properties`) was not reproducible. |

# Open Issues in This Release

These open technical issues merit your review to avoid difficulties.

## Install and Uninstall

| Number | Description |
|---|---|
| 35599<br>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.<br>**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.<br>**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.`"<br>Workaround: Make sure that the Manager is running before you install ArcSight Web. |

| Number | Description |
|---|---|
| 46153 | **On Solaris:** For fresh ESM Manager installations/Manager upgrade, when the solutions packages get installed, occasionally the Manager installation/upgrade does not complete.<br>**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. |
| 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.<br>**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.<br>**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`<br>**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.<br>**Workaround**: Update the logo manually after you upgrade ArcSight Web. See the ArcSight Web *User's Guide* for details on how to do this. |

| Number | Description |
|---|---|
| 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".<br>**Workaround**: Make sure to change the authentication method back to "Password Based and SSL Client Based Authentication". |
| 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.<br>**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.<br>**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:<br>`./arcsight arcdt session-waits -c 1 -f 10 -fmt html -sp -o /tmp/ss.html`<br>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.<br>**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.<br>**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).<br>• Insider Threat Rule, Report, and Query: General Security – User Account Standard Violation<br>**Workaround:** You can remove these resources before or after the upgrade.<br>• Insider Threat Asset: `webproxy.kaxy.com`<br>**Workaround:** Before or after upgrade, add the correct IP address for `webproxy.kaxy.com`<br>• Any Solution Package: NRM – Quarantine rules<br>**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.<br>• PCI Dashboard: AntiVirus Activity Overview<br>**Workaround:** No workaround is necessary as the operation of the dashboard is not impacted<br>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.<br>**Workaround**: Cancel the installation after the Console is installed, and run the ArcSight Console configuration wizard to configure property settings.<br>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:<br>`com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old`<br>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.<br>**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.<br>**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.<br>**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.<br>**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.<br>**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:<br>`No heartbeat response received.`<br>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:<br>`Install Failed: Resource in broker is newer than modified resource.`<br>This error does not occur every time you attempt to install an exported package from a bundle.<br>**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:<br>`[ERROR][default.com.arcsight.server.search.index.IndexResources][_init]`<br>`java.io.IOException: read past EOF`<br>**Workaround**: Regenerate the index by issuing the following command from the Manager `<ARCSIGHT_HOME>/bin` directory:<br>`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.<br>**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.<br>**Workaround**:<br>1 Set the following property in the `<ARCSIGHT_HOME>/config/server.properties` file:<br>`server.date.correction.recoverFromBCDate=true`<br>2 Restart the Manager.<br>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.)<br>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).<br>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.<br>This impacts ESM-TRM (Threat Response Manager) integration commands, as well as other third party integrations.<br>**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.<br>**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.<br>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.<br>The Manager's CPU utilization may become high especially in the kernel CPU utilization area. This issue may be specific to your system/hardware.<br>**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.<br>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.<br>**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.<br>**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.<br>**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.<br>**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:<br>• If there are assets in the channel that are deleted and then re-added or updated.<br>• 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.<br>**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.<br>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.<br>**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.<br>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.<br>**Workarounds:**<br>• 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.<br>• 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.<br>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.<br>**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.<br>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.<br>**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.<br>**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”.<br>**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 Commnads->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.<br>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.<br>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.<br>**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.<br>**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.<br>**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.<br>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.<br>**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.<br>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.<br>**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:<br>1 Log in to the ESM Console, choose **Query Viewers** in the Navigator, and right-click on the query viewer you want to edit.<br>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.<br>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.<br>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.<br>**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.<br>**Workaround**: Start a new session. |
| 56258 | When you create a Case, if you set the Estimated Resource Time, it does not get set.<br>**Workaround**: Define this setting on the Console. See the Console online help for steps to do this. |

## DST Issues

| | |
|---|---|
| 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<br>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.<br>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.<br>**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.<br>**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.<br>**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.<br>**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.<br>**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.<br>**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.<br>**Workaround**:<br>1 Create a package and explicitly include the resources that should never be deleted in the package.<br>2 Export that package.<br>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.<br>**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**.<br>**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.)<br>Running a report or launching a Query Viewer with such a query generates an exception similar to this one:<br>`The query run failed because of the following reason:`<br>`com.arcsight.common.ArcSightException: com.arcsight.common.introspection.queryable.QueryableFetchException:`<br>`Encountered persistence problem while fetching data: Unable to execute`<br>`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)`<br>**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:<br>• an event-based active list with values<br>• a field-based active list with values, where all fields are mapped to event fields<br>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.<br>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)`.<br>This rule will not trigger successfully, and the logs will show an exception indicating ESM is “unable to evaluate rule”.<br>**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.<br>**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:<br>`Exception in thread "main" java.lang.NullPointerException`<br>`at java.util.Hashtable.put(Hashtable.java:394)`<br>`at java.util.Properties.setProperty(Properties.java:143)`<br>`at java.lang.System.setProperty(System.java:731)`<br>`atcom.arcsight.install.wizard.WizardProcessorBase.run(Wiz`<br>`ardProcessorBa`<br>`se.java:118)`<br>`atcom.arcsight.install.wizard.WizardProcessorBase.run(Wiz`<br>`ardProcessorBa`<br>`se.java:89)`<br>`atcom.arcsight.tools.logsender.LogSenderWizard.main(LogSe`<br>`nderWizard.jav`<br>`a:2301)`<br>`Exiting...`<br>**Workaround:**<br>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."<br>**Workaround:**<br>While installing the Connector:<br>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.<br>2 Open a shell/command prompt window.<br>3 Run the following command from `<ARCSIGHT_HOME>/current/bin` directory:<br>`arcsight connector tempca -ac`<br>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.<br>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.<br>**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.<br>**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.<br>**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. |