

Release Notes ArcSight™ ESM

Version 4.5 SP2

February 01, 2010



Release Notes ArcSight™ ESM , Version 4.5 SP2

Copyright © 2010 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

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
02/01/10	ArcSight™ ESM Version 4.5 SP2	Updated the Oracle CPU and OPatch to reflect the January 2010 release of the same. ESM v4.5 SP2 got certified with the Jan 2010 Oracle CPU
01/18/10	ArcSight™ ESM Version 4.5 SP2	Release Notes for ArcSight™ ESM Version 4.5 SP2.

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://protect724.arcsight.com

Contents

ArcSight ESM, Version 4.5 SP2	1
Welcome to ESM v4.5 SP2	1
About Platforms	1
Purpose of this Release	1
Upgrading to ESM v4.5 SP2	1
Installation and Configuration	1
Forwarding Connector	2
Usage Notes	2
Adobe Flash Player Limitation	2
Case Customization	2
Change in Report Output for CSV format	2
Oracle's Dynamic Sampling and Query Performance	3
Logging in as systemuser while using Active Directory or LDAP	3
Geographical Information Update	3
Vulnerability Updates	4
Oracle Critical Patch Update (CPU) Certification	4
OPatch	5
To Apply the CPU	5
Workarounds for Known Issues in Oracle CPU	6
Issues Fixed in v4.5 SP2	7
Upgrade	7
ArcSight Manager	7
ArcSight Console	8
Analytics	10
Localization	10
ArcSight Web	11
Pattern Discovery	11
Issues Remaining Open in SP2	11
Install and Uninstall	11
Upgrade	12
ArcSight Database	14
ArcSight Manager	15
ArcSight Console	18
ArcSight Web	21

DST Issues	22
Analytics	23
Connectors	26
Localization	26

ArcSight ESM, Version 4.5 SP2

Welcome to ESM v4.5 SP2

ArcSight Enterprise Management (ESM) v4.5 introduces a new feature set that broadens its security information and event management functionality. The new capabilities and improvements introduced in v4.5 are significant and varied. Please refer to the *ArcSight ESM v4.5 Reviewer's Guide* and the "What's New" page in the product Online Help.

About Platforms

Please see the official *ArcSight Product and Platform Lifecycles* document for a complete and definitive list of supported platforms for each component.

Purpose of this Release

The purpose of this Service Pack is to:

- update translation packages for Japanese, Traditional Chinese, French, and continue support for Simplified Chinese
- address customer requested and other issues
- Updates for geographical information and vulnerability mapping
- provide Oracle CPU certification with currently available CPU of January 2010 Update

Upgrading to ESM v4.5 SP2

The upgrade for this release is supported from ESM v4.0 SP3 and ESM v4.5 SP1. Please refer to the respective upgrade guides for more information on upgrade instructions.



Caution

If upgrading from an older version of ESM, you are required to upgrade to all the interim versions one at a time, before upgrading to v4.5 SP2.

For example, if you are upgrading from v4.5 GA to v4.5 SP2, you will be required to first upgrade your v4.5 GA installation to v4.5 SP1 before upgrading to v4.5 SP2. See the *Upgrading ArcSight ESM from v4.5 GA to v4.5 SP1* document for details on upgrading to v4.5 SP1. After you have upgraded to v4.5 SP1, see the *Upgrading ArcSight ESM from v4.5 SP1 to v4.5 SP2* document to upgrade to v4.5 SP2.

Installation and Configuration

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

Forwarding Connector

The ArcSight Forwarding Connector 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.

This release supports both FIPs compliant and non FIPs compliant versions of the Forwarding Connector (ArcSight-4.7.6.5416.0-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.

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".

Also see bug "51112" on page 17 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 SP2.

ESM v4.5 SP2 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 to 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 is still not resolved, contact ArcSight Customer Support for help.

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 Enable ArcSight systemuser by running 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.

Geographical Information Update

This release includes an update to the geographical information used in graphical displays. The update version is GeoIP-532_20091201.

Vulnerability Updates

This release includes recent vulnerability mappings (December 2009 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 281	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Enterasys Dragon IDS	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Cisco Secure IDS S457	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
McAfee Intrushield	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
TippingPoint UnityOne DV7859	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Fortinet Fortigate	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
ISS SiteProtector	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Symantec Endpoint Protection	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
McAfee HIPS 7.0	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Radware DefensePro	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
FunkWerk (VarySys Technologies) PacketAlarm	Arachnids, Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB

Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM has been certified with the Oracle critical patch update (CPU) for January, 2010. Certification has been established with Oracle 10.2.0.4. Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

Platform	CPU January 2010 Patch
Windows 32	p9169457_10204_Win32.zip
Windows 64 (AMD64-EM64T)	p9169460_10204_MSWIN-x86-64.zip
Linux 32	p9119226_10204_Linux-x86.zip
Linux x86-64	p9119226_10204_Linux-x86-64.zip
AIX	p9119226_10204_AIX5L.zip
Solaris 64	p9119226_10204_Solaris-64.zip

OPatch

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

Platform	OPatch January 2010
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:
 - ◆ 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:
 - ◆ Review the [README](#) file in the OPatch zip archive.
 - ◆ Extract the contents of the OPatch zip file under `$ORACLE_HOME`.
- 3 Stop the ArcSight Manager and Partition Archiver, and also stop the Oracle instance and TNS Listener.
- 4 Set the OPatch binary in PATH.
- 5 Read the next section in this document, “Workarounds for Known Issues in Oracle CPU” on page 6.
- 6 Install the CPU (that you downloaded in [Step 1](#)) according to the steps outlined in the [README](#) in the CPU zip package for your platform.
- 7 Replace references to “OPatch” in the commands with `$ARCSIGHT_HOME/bin/arcdbutil patch`

where `$ARCSIGHT_HOME` refers to the location where you have installed the ArcSight Database.

For example,

On Windows:

If the [README](#) says:

```
>OPatch apply
```

Then use this command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch apply
```

On UNIX:

If the [README](#) says:

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

Then use this 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 workarounds for issues related to the Oracle CPU on different platforms.

Windows for Oracle 10g

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

```
OUI-67124:Copy failed from "<source>" to "<destination>"  
  
OPatch failed with error code 115
```

This error occurs when there are other processes running that lock the file in question. The processes that cause the lock might be related to Oracle. As a workaround, reboot the machine and try the patch application steps again.

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 between 2 GB and 4 GB of memory (the default configuration of the Large template), 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 the 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.

Restarting the database server 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 v4.5 SP2

The following issues are fixed in this Service Pack. This release includes issues fixed up to and including the Arcsight ESM v4.5 SP1, Patch 3 update.

Upgrade

Number	Description
58406	<p>Upgrade process would fail if sufficient amount of resource cache space was not available.</p> <p>The upgrade process has been enhanced to setup sufficient amount of resource cache space before upgrading resources, thus making the process more robust.</p>

ArcSight Manager

Number	Description
26136	<p>Authentication request from ESM to a RADIUS server was failing. The RADIUS server was generating an error in its authentication response.</p> <p>The product software has been updated to address this issue. An authentication request packet from ESM did not contain a NAS IP Address or a NAS identifier, thus causing the RADIUS server to generate an error and fail the authentication request. The updated product software includes this information in the authentication request.</p>
47455	<p>The notes associated with a package were not exported when the package was exported.</p> <p>The product software has been enhanced to export notes associated with a package when it is exported.</p>
54437	<p>When the ESM Manager Asset belongs to a Customer Network, the customer URI field in the events received from the connectors and the correlated events generated on the Manager for the customer network would be overwritten.</p> <p>The product software has been updated such that the customer URI is not overwritten.</p>
56812	<p>On Red Hat Linux 5.3: After rebooting the system, the Manager, Web, and Partition Archiver services did not start automatically.</p> <p>This issue has been fixed.</p>

Number	Description
58400 58401	<p>If a very large number of resources were configured on a Manager, the search index and resvalidate processes would either take a long time to complete or would fail due to insufficient memory. As a result, the upgrade process would fail.</p> <p>The timeout value has been increased to accommodate a longer running search index or resvalidate process during the upgrade.</p>
59366	<p>An ESM Manager would not start up if the "Device Asset Auto Creation Controller" filter was modified such that it contained one or more "Device Zone != <IP_address_range>".</p> <p>The product software has been updated to address this issue. Modifying the filter does not prevent the Manager from starting up.</p>
63236	<p>When receiving forwarded events, the destination Manager may trigger the <code>MaxEventIdExceededCheckTask</code> because event ids for forwarded events exceed the 48 bits used to store local event IDs. Subsequently, the destination Manager would stop accepting events.</p> <p>This issue has been fixed.</p>

ArcSight Console

Number	Description
52792	<p>A search operation was not limited to the specified resource types when the operation was run from the Search Field on the Console tool bar.</p> <p>The product software has been updated to address this issue. Now, the search is limited to the selected resource type.</p>
52938	<p>After upgrading ESM to 4.5, some dashboards may appear as broken although they are functional. A tool has been provided to clean up those dashboards, should they appear.</p> <p>To "clean up" these dashboards, run <code>arcsight resfixup</code> from the command line.</p>
53737	<p>When a user tried to modify a case while a case channel was open and sorted based on an Integer field, such as case id, a java Runtime Exception occurred.</p> <p>This issue has been fixed.</p>
55367	<p>Notification messages were not displaying on the Console.</p> <p>The product software has been updated to address this issue. The notification messages display as pop-up windows on the Console.</p>
55907 56560	<p>Some drop-down menus would not work as expected on the ESM Console running on Mac OS X. For example, left-mouse button would not select the item, but the right-mouse button would.</p> <p>The product software has been updated such that the menus work as expected on Consoles running on Mac OS X.</p>

Number	Description
56034	<p>When you tried to remove or override status of an entry from a dashboard for "Last State Data Monitor" by right-clicking the entry, the confirmation message window displayed the name of a different node than the one on which you were trying to operate. This issue was observed only when the dashboard information had been sorted by any of the columns displayed in it. The issue did not exist if the information was unsorted.</p> <p>The product software has been updated to address this issue. The confirmation message window displays the correct name of the node now.</p>
56093	<p>When a user tried to modify a case while a case channel was open and an inline filter was applied to the channel, a java Runtime Exception occurred.</p> <p>This issue has been fixed; however, after modifying a case, the case channel should be refreshed.</p> <p>See also, 61659.</p>
56275	<p>When a user tried to update a case previously configured for automatic updating, the operation would sometimes fail. When this occurred, an error message would appear and the case required another update.</p> <p>The product software has been updated to address this issue.</p>
58475	<p>When a custom banner was used for the ESM Console login, the "User Access Log" dashboard would display a "Login Failed for user name <user_name>" status for a user who had successfully logged in.</p> <p>The product software has been updated to address this issue. The login status is correctly displayed for custom banner ESM Consoles.</p>
59099	<p>In ESM v4.5 SP1, when the user account of a recipient of a report (sent through e-mail) was deleted, the remaining recipients of that report were not displayed in the drop-down menu of the "Email to" field in the Report Parameters tab.</p> <p>The product software has been updated to address this issue. The remaining recipients are now displayed as expected.</p>
59258	<p>No data would be returned when a filter was defined on the "deviceDirection" field in the Trend Data Viewer.</p> <p>The product software has been updated to address this issue. Now the filter works as expected.</p>
59310	<p>If all fields of an active list referenced in a filter were not mapped in the filter definition, the mapped fields were not displayed in the filter editor. (Note that the conditions specified in the filter worked as expected, even when the mappings were not displayed.) If all fields of the active list were mapped, the Filter editor displayed the mappings.</p> <p>The product software has been updated to address this issue. The Filter Editor displays mappings even when only the key fields are mapped.</p>
60181	<p>Unexpected value was applied to a session list expiration time instead of the entered value for some values.</p> <p>The product software has been updated to address this issue. The entered value is appropriately applied and used.</p>

Number	Description
61512	The process of batch editing cases from the case channel now works similarly to that of the case resource tree. This issue has been fixed.
61545	Query Viewer did not support "Annotate Events" and "Show Event Details" options. The product software has been enhanced to include these options.

Analytics

Number	Description
60243	During execution of an integration command, quotes were automatically added to values that contain spaces, but not for values that contain a character (for example, values from the <code>deviceEventClass</code> field). This issue caused problems for ESM Logger integration, in which values that contain but not quoted are treated as regular expressions. The product software has been updated to address this issue.

Localization

Number	Description
41950	If the name of a notification group was modified in the Navigator panel, the updated name was not displayed in the rule definition (in the TargetGroup field) that references the group. The product software has been updated to address this issue. Now, the updated name is displayed in the rule definition.
46627	Localization package (LU2) could not be applied to an ESM system running on a Windows 2003 R2, 64-bit, Simplified Chinese machine. The product software has been updated to address this issue. Now, the localization packages can be applied to the system with the above listed specifications.
60311	When a value that includes a comma (,) or is enclosed in double quotes (") is imported into an active list using the "import CSV" function, a trailing double quote (") is added to the imported value. For example: CSV file contains: <code>"cn=user ,dc=xx ,dc=com", "user"</code> the values are imported as <code>cn=user ,dc=xx ,dc=com</code> and <code>user"</code> This issue has been fixed.

ArcSight Web

Number	Description
58051	Custom column names in an ArcSight Web Active Channel would not display. The product software has been updated to address this issue.

Pattern Discovery

Number	Description
58178	When a snapshot was created for Pattern Discovery and values were repeated in mixed case, it would sometimes fail with the following error: <code>RuntimeError : Default Transaction builder sees repeated supporter!</code> The product software has been updated to address this issue.

Issues Remaining Open in SP2

The following issues are carried forward from ESM releases and remain open in v4.5 SP2. These open technical issues merit your review to avoid difficulties.

Install and Uninstall

Number	Description
35599	When performing ArcSight Database installation and you are prompted for directories for the <code>REDO</code> or <code>SYSTEM</code> volumes, entering directories that do not exist halts installation and an error appears. Workaround: Make sure that the directories for the <code>REDO</code> or <code>SYSTEM</code> volumes exist before installing the database. Create them, if needed.
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 <code>runconsolesetup.sh</code> in the console mode, you will see an error message, <code>"chmod: cannot access `/arcsight/Console5199/current/config/console.properties" : No such file or directory"</code> . 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, <code>"Could not log in. The ArcSight Manager has a different version than your client."</code> Workaround: Make sure that the Manager is running before you install ArcSight Web.

Number	Description
46153	<p>On Solaris: When performing a fresh ESM Manager installation/upgrade, the installation/upgrade does not always complete when solutions packages are installed.</p> <p>Workaround: 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 to ensure that your system meets the minimum requirements.</p>
47129	<p>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.</p>
50562	<p>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.</p> <p>Workaround: Delete the link manually.</p>
51954, 52680, 52690, 54003	<p>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.</p> <p>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.</p>
55853	<p>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:</p> <p><code>error ORA-00921: unexpected end of sql command</code></p> <p>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.</p>

Upgrade

Number	Description
25121	<p>If you used a custom logo for ArcSight Web, the logo may not show up correctly when you upgrade ArcSight Web.</p> <p>Workaround: Update the logo manually after you upgrade ArcSight Web. See the <i>ArcSight Web User's Guide</i> for details on how to do this.</p>

Number	Description
47206	<p>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".</p> <p>Workaround: Make sure to change the authentication method back to "Password Based and SSL Client Based Authentication".</p>
51319	<p>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.</p> <p>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., <code>C:\arcsight\db</code>). 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.</p>
52394	<p>File resources are not handled properly during ESM upgrading. This results in unassigned file resources after the upgrade. For example, <code>.art</code> 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.</p> <p>Workaround: You can remove the unassigned <code>.art</code> files after an upgrade, since they are duplicates. The <code>.art</code> files can be safely deleted.</p>
34527	<p>The <code>arcdt</code> 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:</p> <pre>./arcsight arcdt session-waits -c 1 -f 10 -fmt html -sp -o /tmp/ss.html</pre> <p>This is caused by an issue with the JDBC driver.</p>
42536	<p>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.</p> <p>Workaround: Wait until 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).</p>

Number	Description
55935	<p>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.</p> <p>Workaround: Cancel the installation after the Console is installed, and run the ArcSight Console Configuration Wizard to configure property settings.</p> <p>In <code><ARCSIGHT_HOME>/<Console_Build>/current/bin</code>, run the <code>arcsight consolesetup</code> at the command line. This way, SSL files are read and the Console can configure correctly.</p>
61714	<p>On Unix only: When upgrading from ESM 4.5 SP1 Patch 2/Patch 3, to ESM 4.5 SP2, the dbcheck script produces an error.</p> <p>Workaround: Do the following before running the <code>arcsight dbcheck</code> command:</p> <ol style="list-style-type: none"> 1 Open a shell window and go to the Database's <code><ARCSIGHT_HOME>/bin/scripts</code> directory. 2 Run the <code>dos2unix dbcheck.sh</code> command.
62801	<p>When upgrading from <i>ESM 4.5SP1/ESM 4.5 SP1 Patch1/Patch 2/Patch 3</i>, to ESM 4.5 SP2, customized shortcut keys disappear from the Console UI.</p> <p>Workaround: To make shortcut keys reappear, do the following:</p> <ol style="list-style-type: none"> 1 Stop the Console. 2 Manually copy <code><ARCSIGHT_HOME>/config/console/keymap.xml</code> from <i>ESM 4.5SP1/ESM 4.5 SP1 Patch1/Patch 2/Patch 3</i> installation folder to the corresponding location in your v4.5 SP2 installation. 3 Restart the Console.

ArcSight Database

Number	Description
53484	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <pre>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</pre> <p>This occurs because Oracle is using a sub-optimal query execution plan. In some cases, this can happen because of insufficient space in the <code>ARC_TEMP</code> table as well.</p> <p>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 <i>ArcSight ESM Administrator's Guide</i>.</p>
56718	<p>The <code>dbcheck</code> utility fails to create a <code>.zip</code> file for its logs on Windows as indicated in the upgrade guide.</p>

Number	Description
57116	<p>On the Solaris platform: Occasionally, the following error displays when you try to create a database instance.</p> <p>Database test connection failed. ORA-07445: exception encountered: core dump [kgskhighthreshold()+72] [SIGSEGV]</p> <p>This is due to an issue described in Oracle ticket number Doc ID 805206.1. If you encounter this error, contact ArcSight Customer Support for assistance.</p>

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	<p>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.</p> <p>Workaround: Exit the Send Logs utility and restart it after freeing disk space on your machine.</p>
36553	<p>Windows only: The command line tools <code>arcsight managersvc start</code> and <code>arcsight managersvc stop</code> are not supported for this version of the product.</p> <p>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.</p>
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 may be unpredictable.
39988	<p>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.</p> <p>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.</p>
41193	<p>On Solaris, in a high availability environment, when you execute the <code>arcsight managerup</code> command, even if the Manager is running, you will see the following incorrect message:</p> <p><code>No heartbeat response received.</code></p> <p>Ignore this message as this will appear even though the Manager is running.</p>

Number	Description
41582	<p>Occasionally, when installing an exported package from a bundle file, you might receive the following error:</p> <pre>Install Failed: Resource in broker is newer than modified resource.</pre> <p>This error does not occur every time you attempt to install an exported package from a bundle.</p> <p>Workaround: Re-import the package.</p>
42502	<p>On a Manager with a large number of assets (e.g., 800,000), selecting the Stop button in the Console when a recursive Asset channel is showing, then restarting it, results in a communication error.</p>
42730	<p>You cannot move an asset using Auto Zone if the asset is locked.</p>
43678	<p>If the search index file becomes corrupted, the Search index will be out-of-date and the following message appears in the Manager log:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Regenerate the index by issuing the following command from the Manager <ARCSIGHT_HOME>/bin directory:</p> <pre>arcsight searchindex -a create</pre>
47345	<p>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.</p> <p>Workaround: Make sure to set your Manager's Java Heap Memory size to less than half of the physical RAM available on your system.</p>
50794	<p>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.</p>
51053	<p>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. The resources for this error are not loaded.</p> <p>Workaround:</p> <ol style="list-style-type: none"> Set the following property in the <ARCSIGHT_HOME>/config/server.properties file: <pre>server.date.correction.recoverFromBCDate=true</pre> Restart the Manager. <p>Should this issue occur, notify ArcSight Customer Support so that they can investigate its cause within your setup.</p>

Number	Description
51112	<p>Stages resources are editable from the ESM Console, although these should not be moved or customized. (See ESM Console Navigator > Stages resource tree.)</p> <p>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 "Standard Content" topic in the Console Help.)</p>
51134	<p>ESM integration commands launched from a chart view cannot pick up attribute values from the chart (as they can from grid views).</p> <p>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.</p> <p>This impacts ESM-TRM (Threat Response Manager) integration commands, as well as other third party integrations.</p> <p>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.</p>
53975	<p>User is unable to set up sending pager notifications through the pager service provider.</p> <p>Workaround: If the 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.</p>
54452	<p>A <code>java.lang.InterruptedException</code> might be logged in the ESM Manager <code>server.std.out.logs</code> when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager.</p> <p>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.</p>
55969	<p>On Linux only: The ESM Manager CPU utilization is higher than expected and impacts performance.</p> <p>The Manager's CPU utilization may become high especially in the kernel CPU utilization area. This issue may be specific to your system/hardware.</p> <p>Workaround: It may be possible to fix this issue by updating drivers or reinstalling the Linux operating system.</p>
56466	<p>Pattern Discovery still causes some unnecessary full garbage collection cycles on the Java Virtual Machine (JVM). This is done to ensure support for memory usage required by large data sets.</p>
56556	<p>There is no way to specify a NULL value for "preview" input to a Variable function on the Console Common Conditions Editor (CCE). The Preview assumes that a blank field for an input is an empty string. Therefore, you cannot use the Preview function on the Variable dialog to test inputs for a parameter with NULL values.</p> <p>This is expected behavior which will be documented in the 5.0 release.</p>

Number	Description
57324	<p>If a column name in the Active List contains more than 30 characters, you see an error message. ArcSight has reworded this error message so that it is easier to understand.</p> <p>Workaround: Make sure that the column name contains fewer than 30 characters.</p>
59212	<p>On Macintosh: When you install the ArcSight Console Patch, customized content for</p> <p><code><ARCSIGHT_HOME>\i18n\common\label_strings.properties</code> and <code><ARCSIGHT_HOME>\i18n\common\resource_strings.properties</code> files is not merged from your previous installation.</p> <p>Workaround: After you install the ArcSight Console Patch, copy customized content, if any, from the backup of your previous installation (for example, Patch 4).</p>
61227	<p>The -u resource is not an option for export, when running the ESM archive tool with the following command:</p> <pre>arcsight archive -u <username> -m <source_manager_hostname> -format exportuser -f exportusers.xml</pre> <p>Workaround: The -u option can be used if the archive tool is run in standalone mode.</p>

ArcSight Console

Number	Description
24496	<p>Drill down from Event Graph data monitors to channels is not supported when the Event Graph data monitor uses Variables to retrieve or parse event information.</p>
38270	<p>While installing a package, if you cancel the installation before it is completed, the Import button is disabled.</p> <p>Workaround: Refresh the Console or log in to the Console again to enable this button.</p>
40627	<p>In the standard field set for a channel, changing the Column Flip Limit in the Preferences dialog does not take effect after clicking Apply or OK.</p> <p>Workaround: In order for the new value to take effect, press the Enter key before you click Apply or OK.</p>
41305	<p>When a custom column in an Active Channel uses the "\$fieldname notation", you will see the "\$fieldname" value in the cell if the value of the field is null.</p>
42538	<p>Performing unrelated UI operations in the Console after launching bulk asset operations (such as bulk Vulnerability assignments) can cause the operation to abort.</p> <p>Workaround: To avoid any possible problems, allow the bulk asset operation to complete before performing any further work in the Console UI.</p>
42859	<p>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.</p>

Number	Description
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.
44028	On Macintosh: If you click the Help menu and select About and then click the ArcSight Copyrights... link in the "About" page, you will get a Java Exception. This 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: <ul style="list-style-type: none"> • 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.
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.

Number	Description
51245	<p>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.</p> <p>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.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>This is a harmless issue, so you can continue by clicking the one you want to select.</p>
52617	<p>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.</p> <p>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.</p>
52626	<p>Although available in Acrobat Reader 6, the Japanese font (KozMinPro-Regular-Acro.otf) is not available in Acrobat Reader 8.</p> <p>Workaround: use an alternative font available in Acrobat Reader 8 or switch to a report format such as HTML.</p>
52926	<p>When specifying attributes within the Console where a panel or resource editor has multiple resource selector drop-down menus, the drop-down menu for an attribute may display the drop-down menu of the previously selected attribute. For example, if you selected Location followed by Zone, the drop-down menu for Zone displays the menu list for Location instead.</p> <p>Workaround: Click a node within the resource selector drop-down menu. This refreshes the view of the selected attribute.</p>

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.
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.
59649	Linux and Mac OS: Logger integration commands are not available from the context menu on the Channels tab of the ArcSight Console. Workaround: To run Logger integration command for these operating systems, use an external browser.
61659	When a user tries to modify a case while a case channel is open and an inline filter is applied, no data appears. Workaround: To successfully display available data, refresh the case channel. See also, 56093 .
61713	On ESM 4.5 SP1, if the "\" character is used on a rule condition, the rule fails to compile. An error message appears. 4.0 SP3 does not have this problem. As a result, if you perform an upgrade from 4.0 SP3 to 4.5, all the rules that have "\" in the their conditions are broken. Workaround: Specify the condition in a filter and use the filter in the rule condition (instead of specifying this condition directly in the rule.)

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 Web server 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 Web server is connected. This feature is not supported for this release of the product.
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, they do not appear. Workaround: Restart ArcSight Web.

Number	Description
43327	<p>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 produces an error.</p> <p>Workaround: Use ArcSight Console to modify the channel sort column and then use it in ArcSight Web.</p>
46969	<p>When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an Active Channel.</p>
52336	<p>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.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 1 Log in to the ESM Console, choose Query Viewers in the Navigator, and right-click 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.
56258	<p>When you create a Case, if you set the Estimated Resource Time, it does not get set.</p> <p>Workaround: Define this setting on the Console. See the Console online Help for steps to do this.</p>

DST Issues

Number	Description
54713	<p>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.</p>
54749 55835	<p>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.</p>

Analytics

Number	Description
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	<p>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.</p> <p>Workaround: To improve readability when sections contain more than a page of data, we recommend setting the vertical alignment of the relevant section column to the top. This causes the value of the section to appear at the top of the relevant section, making the report more readable.</p>
36051	<p>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.</p> <p>Workaround: Refine your search criteria to be more specific and retry the search.</p>
36148	<p>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.</p> <p>For example, to search for <code>^VVsoXg4BABCAIEuBhILMyg==</code>, enter <code>"^VVsoXg4BABCAIEuBhILMyg=="</code> in the Query text field.</p>
38832	<p>When you display Assets in an Asset Channel, the Device Zone Network Name column does not get populated in the Grid view.</p> <p>Workaround: To view the details of an Asset, click the right-facing arrow in the first column to open the Asset Detail box.</p>
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	<p>When applying a new channel to verify rules, the generated events may not show up in the channel correctly because the correlated events don't match the filter.</p> <p>Workaround: Add an OR condition to the channel filter as "sessionID > 0" when you specify a filter for testing rules with replay.</p>
40230	<p>After editing the description for a trend, if another trend is dependent on it, the dependent trend becomes invalid.</p> <p>Workaround: Disable the dependent trend in the trend editor, then re-enable it.</p>

Number	Description
43456	<p>When creating an asset, assigning a category to it, and adding the asset to a new package, uninstalling the package results in the category also being deleted.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1 Create a package and explicitly include the resources that should never be deleted in the package. 2 Export that package. <p>If the resources under the parent groups change, then that package may need to be exported periodically.</p>
43912	<p>If you import the content of an older package into an existing newer package, the contents from the two packages are merged. The resulting package will consist of contents from both packages. The relationships are merged, but the attributes are picked up from the old package.</p> <p>Workaround: Export the new package to a bundle file so that you can recover if needed. Then delete the new package before importing the old one.</p>
50646	<p>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.</p> <p>Workaround: Create only short aliases for such columns in the report editor.</p>
51280	<p>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.)</p> <p>Running a report or launching a Query Viewer with such a query generates an exception similar to this one:</p> <p>The query run failed because of the following reason:</p> <pre>com.arcsight.common.ArcSightException: com.arcsight.common.introspection.queryable.QueryableFetchException: 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)</pre> <p>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.</p>

Number	Description
54507	<p>Verify Rules with Events (replay with rules) does not work for these types of active lists:</p> <ul style="list-style-type: none"> an event-based active list with values a field-based active list with values, where all fields are mapped to event fields <p>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.</p>
55314	<p>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.</p> <p>For example, consider a Rule with a condition that compares the JME argument <code>sqr(4)</code> to a variable named <code>abc-cde</code>, where the value of <code>abc-cde</code> is: <code>add (2.0,3.0)</code>.</p> <p>This rule will not trigger successfully, and the logs will show an exception indicating ESM is "unable to evaluate rule".</p> <p>Workaround: As a best practice, do not use dashes or hyphens (-) in variable names. Underscores (_) are acceptable in variable names, but upper and lower case letters only are best.</p>
56345	<p>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.</p>
59649	<p>Linux and Mac OS: Logger integration commands are not available from the context menu on the Channels tab of the ArcSight Console.</p> <p>Workaround: To run Logger integration command for these operating systems, use an external browser.</p>
60305	<p>The Integration command does not pick up values using an event-based field name if the context is an active list or a session list.</p>
61576	<p>When using a Query Viewer, if you drill down on a resource reference field, the drilldown menu may not show up. You may also see an exception.</p>
61885	<p>ESM does not support the modification of the Active List schema (the ArcSight Console prevents this action). Importing a new schema for an Active List through archives can lead to inconsistencies in the Active List schema definition and table.</p> <p>Workaround: If you feel that you have inadvertently modified your Active List schema by importing an Active List with the same URI but different schema, please call ArcSight Customer Support to correct this issue.</p>
62843	<p>Installation of SOX 4.0 on ESM 4.5SP1 may result in Console dashboards and other resources "breaking" within the Navigator.</p> <p>Workaround: To fix these resources, run the following script:</p> <pre>arcsight resfixup -u <user> -p <password> -m <manager_name> -port <port number></pre>

Connectors

Number	Description
45785	<p>The Asset Import SmartConnector ignores the category content in the second CSV entry (with the same IP address) if a duplicate asset is imported.</p> <p>Workaround: To avoid creating a duplicate asset for the imported asset, complete all required category URLs in a single CSV entry.</p>
46902	<p>Running <code>arcsight agent sendlogs</code> command from the connector's <code><ARCSIGHT_HOME></code> when the connector is installed in FIPS mode results in the following error:</p> <pre>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) at com.arcsight.install.wizard.WizardProcessorBase.run(WizardProcessorBase.java:118) at com.arcsight.install.wizard.WizardProcessorBase.run(WizardProcessorBase.java:89) at com.arcsight.tools.logsender.LogSenderWizard.main(LogSenderWizard.java:2301) Exiting...</pre> <p>Workaround: Use the sendlogs feature by clicking Tools->Sendlogs in the Console.</p>
47377	<p>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 <code>agent_error_batch*<AgentID>.bin</code> files under the Manager's <code>logs/default</code> directory.</p> <p>Ignore these files as they do not cause any data loss.</p>

Localization

This section provides information on related open issues.

Number	Description
45090	<p>A field (Data Monitor Type) in the Attribute tab of Data Monitor Editor is only partially displayed.</p> <p>Workaround: Expand the Inspect/Edit pane until you see the full text in the Data Monitor Type field.</p>
45278	<p>On Solaris, when you generate a report in the PDF format, the contents of the report appear to be garbled.</p> <p>Workaround: Generate the report in a format other than PDF.</p>
46242	<p>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.</p>

Number	Description
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	<p>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.</p> <p>Workaround: Use other formats such as HTML, CSV, etc. to generate reports.</p>
55823	In Traditional Chinese and Japanese environments: Assigning a hotkey to a resource is not supported for this release.

