

Release Notes ArcSight™ ESM

Version 5.0 SP2

September 2011



Release Notes ArcSight™ ESM Version 5.0 SP2

Copyright © 2011 ArcSight, LLC. All rights reserved.

ArcSight and the ArcSight logo are registered trademarks of ArcSight in the United States and in some other countries. Where not registered, these marks and ArcSight Console, ArcSight ESM, ArcSight Express, ArcSight Manager, ArcSight Web, ArcSight Enterprise View, FlexConnector, ArcSight FraudView, ArcSight Identity View, ArcSight Interactive Discovery, ArcSight Logger, ArcSight NCM, SmartConnector, ArcSight Threat Detector, ArcSight TRM, and ArcSight Viewer, are trademarks of ArcSight, LLC. 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/copyrightnotice>

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
9/27/11	ArcSight™ ESM Version 5.0 SP2	Release Notes for ArcSight™ ESM Version 5.0 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 5.0 SP2	1
Welcome to ArcSight ESM Version 5.0 SP2	1
What's New in This Release	1
Oracle 11G Support	1
Standard Content	1
Upgrade Support	1
Geographical Information Update	2
Vulnerability Updates	2
Usage Notes	2
Oracle Password Expiration Issue	2
Important AIX Issue	3
Embedded and External Browsers	3
Browsers and Custom View Dashboards	3
Scheduled Tasks	4
Getting an Error Message During an Upgrade	4
System Table Import and Export - Oracle 11g	5
System Table Export - Oracle 10g	5
Fixed Issues in v5.0 SP2	6
Analytics	6
ArcSight Console	6
ArcSight Database	7
ArcSight Manager	8
ArcSight Web	9
General	10
Installation and Upgrade	10
Localization	11
Open Issues in v5.0 SP2	11
Analytics	11
ArcSight Console	12
ArcSight Database	12
ArcSight Manager	13
Installation and Upgrade	13
Localization	14
Issues Remaining Open From v5.0 SP1	15

Analytics	15
ArcSight Console	18
ArcSight Database	23
ArcSight Manager	24
ArcSight Web	26
Connectors	27
Installation and Upgrade	28
Localization	31
Pattern Discovery	31

ArcSight ESM Version 5.0 SP2

Welcome to ArcSight ESM Version 5.0 SP2

ArcSight Enterprise Security Management (ESM) v5.0 SP2 improves the feature set for its security and event management platform and its identity correlation functionality.

What's New in This Release

This section contains a summary of the improvements and new capabilities introduced as part of the ArcSight ESM v5.0 Service Pack 2 release.

The Oracle Patch Set Update (PSU) and OPatch information is in separate release notes entitled ArcSight Oracle Patch Set Update (PSU) Release Notes.

This release provides JRE 16.0_26.

Oracle 11G Support

ESM v5.0 SP2 introduces Oracle Database 11g Release 2 for fresh installations, which supports upgrading from existing Oracle 10g on all supported platforms.

See the ESM Installation and Configuration Guide.

Standard Content

ESM v5.0 SP2 includes new and updated standard content packages.

- The ArcSight Administration Foundation Package monitors the function of ArcSight components. It now has updated Connector-Monitoring content, which includes connection and caching status for SmartConnectors.
In the ESM Administrator's Guide, see Appendix H, "Monitoring System Health" and find the topic "ESM Content Configuration" > "Configure Connector Monitoring Resources."
- The NetFlow Monitoring Foundation Package leverages NetFlow session-level data to monitor and report on top bandwidth usage by source, destination and port.
The NetFlow Monitoring Guide is available for download from the ArcSight Customer Support site.

Upgrade Support

The following upgrade paths are supported for this release:

- ESM v5.0 Patch 1 to v5.0 SP2
- ESM v5.0 SP1 Patch 3 to v5.0 SP2

Please refer to the respective upgrade guide for more information on upgrade instructions.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20110801.

Vulnerability Updates

This release includes recent vulnerability mappings (August 2011 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 388	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Enterasys Dragon IDS	Faultline, CVE, MSSB
Cisco Secure IDS S588	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP 1969	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, CERT, MSSB
TippingPoint UnityOne DV8243	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Fortinet Fortigate	Bugtraq, Nessus, MSSB
ISS SiteProtector	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
McAfee HIPS 7.0	Faultline, CVE
Radware DefensePro	CVE X-Force, Nessus, MSSB

Usage Notes

ESM v5.0 SP2 introduces some improvements to existing features. There are a few things to consider when using these features. Please review the following points to ensure smooth operation.

Oracle Password Expiration Issue

Starting with 11g, by default, Oracle has set the passwords to expire 180 days after the account has been created. This causes connectivity issues to the database after the 180 day default period on both new installs as well as on upgraded systems.

This was not the case with Oracle 10g.

If you run into this problem of expired password, then do the following to set the password to never expire.

- 1 `% arcdbutil sql`
- 2 Enter user-name: / as sysdba

- 3 SQL> select PROFILE from dba_users where username =
'<arcsight_schema_owner>';
- 4 SQL> alter PROFILE <profile result from step 3> limit
PASSWORD_LIFE_TIME UNLIMITED;
- 5 SQL> exit;

In 11g, by default, Oracle has set the failed login attempts value to 10. If the account gets locked for exceeding the number of failed login attempts, use the following to resolve the issue.

- 1 % arcdbutil sql
- 2 Enter user-name: / as sysdba
- 3 SQL> alter user <arcsight_schema_owner> account unlock;
- 4 SQL> exit;

For more information on changing this behavior, refer to the knowledge base article KB 5205, which is available from the ArcSight support portal at <https://support.arcsight.com>.

Important AIX Issue

On AIX, run the following commands on the command line immediately after the database instance creation step. These prevent an issue with the partition archiver, in which you get the error "Unable to create archive file" in the agent.log.

```
prompt > arcdbutil sql
SQL>conn / as sysdba
SQL>ALTER SYSTEM set filesystemio_options=ASYNCH scope=spfile;
SQL>shutdown immediate;
SQL>startup
SQL> show parameter filesystemio_options
//output should print ASYNCH as the value
SQL>exit
```

Embedded and External Browsers

The Console's embedded browser is not supported on the following platforms:

- Red Hat Linux 5
- 64-bit Macintosh
- 64-bit Windows

On 64-bit platforms, use the 32-bit version of the browser. This limitation is due to lack of Adobe Flash Player support on 64-bit systems. Consider using an external browser instead, and use the 32-bit version of the browser. You select the browser at installation time or change it in your Console's Preferences menu.

Refer to the following site for more information about the Adobe Flash Player plugin and 32-bit browsers:

<http://kb2.adobe.com/cps/000/6b3af6c9.html>

Browsers and Custom View Dashboards

With dashboards in custom view mode, the dashboard may not launch or charts are not displayed. This is because the Adobe Flash Player is required and you are either using the embedded browser or the 64-bit external browser. If you are using a 64-bit browser, change that to 32-bit in your Console's Preferences menu and then download Adobe Flash Player.

If you are using an embedded browser, download Mozilla Firefox 2 or 3, then restart the Console. The embedded browser copies the Adobe Flash Player from Firefox. You need not change any Preference settings in this case. You may continue to use Internet Explorer and uninstall Firefox if you want.

Refer to the following site for more information about the Adobe Flash Player plugin and 32-bit browsers:

<http://kb2.adobe.com/cps/000/6b3af6c9.html>

Scheduled Tasks

If the trigger time for a particular scheduled task run happens to fall during the transition time from daylight savings time (DST) to standard time (ST) or vice versa, the interval for that particular run will not be the expected interval.

Time zones that honor DST have a period of time that occurs twice during the transition from DST to ST. For example, in the US when changing from DST to ST, this hour occurs once while the DST is still in effect and again after switching to the Standard Time. The transition period occurs at 2 am, therefore 1:00:00 am - 1:59:59 am occurs twice (1:00:00 am PDT - 1:59:59 am PDT and 1:00:00 am PST - 1:59:59 am PST), where 1:00 am PST is 60 minutes after 1:00 am PDT. In this example, if the scheduled task is due to trigger any time between 1:00:00 am - 1:59:59 am, the interval for that particular run of the scheduled task will not be as expected.

Similarly, when the time changes from ST to DST, the 1:00:00 am - 1:59:59 am hour does not occur at all. The local time changes directly from 12:00 am to 2:00 am. So, if your scheduled task run was scheduled to trigger between 1:00:00 am - 1:59:59 am, the interval for that particular run will be off by an hour.

The interval calculation for subsequent scheduled runs do not get affected.

Currently, there are four time zones that are not supported in ESM:

- Kwajalein
- Pacific/Kwajalein
- Pacific/Enderbury
- Pacific/Kiribati

These time zones fall in two countries, Marshall Islands and Kiribati.

Getting an Error Message During an Upgrade

During an upgrade, you might get an error message similar to the following:

Could not create new group for URI filing: Group <name of the group> already contains a node with the same name as resource with id <resource ID>.

It probably means that you have a group in your pre-upgraded system that has the same name and URI as a system resource. To solve this problem, rename that group in your pre-upgraded system and try the upgrade step again.

System Table Import and Export - Oracle 11g

The Oracle 11g import and export utilities require a different mechanism for generating the system table dump file (`ArcSight.dmp`). Therefore the dump file generated with ESM v5.0 SP1 Patch 3 or later is not compatible with the dump files generated with earlier releases.

Use the `import_system_tables` and `export_system_tables` utilities as outlined in the following examples. For additional information see the ESM Administrator's Guide for ESM 5.0 SP2.

```
$ARCSIGHT_HOME/bin/arcsight export_system_tables
<username>/<password>@<TNSName>
```

Export places `arcsight.dmp` in `<ARCSIGHT_HOME>`. Make sure it is still there before doing an import (for example, if you moved it or obtained another one).

```
$ARCSIGHT_HOME/bin/arcsight import_system_tables <export_username>
<import_username> <import_password> <TNSname> <dump_file_path>
<dump_file_name>
```

where `<dump_file_name>` is the full path to find the dump file and
`<dump_file_name>` is `arcsight.dmp` file.

System Table Export - Oracle 10g

When you ran the ArcSight `export_system_tables` script, you might have received the following error:

Error "ORA-39071: Value for TABLES is badly formed."

This is due to an Oracle issue with the `expdp` command of Oracle v10.2.0.4. With this Oracle issue, a 10.2.0.4 `datapump` export using transportable tablespaces with a long list of tablespaces fails with ORA-39071 [ID 1131484.1]. To fix the error, set the compatible parameter on the database to 10.2.0.4.



Note

This fix requires you to schedule a database outage and restart the database.

To fix the error, set the compatible parameter on the database to 10.2.0.4.

- 1 Log in to your database server as an Oracle Software Owner.
- 2 Navigate to `<ARCSIGHT_HOME>/db/bin` and `sqlplus` as `sysdba`.
- 3 Execute the following SQL statements:

```
alter system set compatible = '10.2.0.4' scope=spfile;
shutdown immediate;
startup;
```

- 4 To check if the parameter has been set as required, execute the following statement on the SQL prompt:

```
show parameter compatible
```

Example:

```
SQL> show parameter compatible
```

NAME	TYPE	VALUE
compatible	string	10.2.0.4

- Restart the database.

To track the progress on this Oracle issue, ArcSight has also filed internal bug ESM-47738.

Fixed Issues in v5.0 SP2

Analytics

Issue	Description
ESM-47767	ESM Manager disabled previously-disabled rules with an error that the number of correlated alerts created was too high. This no longer occurs.
ESM-47679	Currently, for Data Monitors that provide the ability to GroupBy specific fields, you can group by any Customer related fields such as Customer Name, Customer URI, and so on. All these options are disabled except for the Customer Resource.
ESM-46869	When using the RequestUrlHost as a field in a Trend, the length of the column created is 64 characters. This was too short and did not match the length of similar fields in the event. Now all fields are 1023 characters.
ESM-39371 TTP#64333	In the ArcSight ESM User's Guide, The following sentence should have been deleted from pages 138 and 289: "Also, query viewers and channels display list results differently. Query viewers display lists the way reports do: one line for each list entry while channels display lists the way data monitors do: [entry1, entry2, entry3]." List results are displayed the same for both.

ArcSight Console

Issue	Description
ESM-48132	The ArcSight Integration Commands do not work because the character encoding is not being parsed correctly. Apply the following changes to enable the ArcSight Integration Commands to work: <ol style="list-style-type: none"> In the console.properties file, set ui.integration.url.encode=false. make a soft link from the xulrunner directory in the /usr/lib64 directory to <ARCSIGHT HOME>/Console/current/lib/xulrunner-linux.

Issue	Description
ESM-47643	<p>If you edited severity filters for a specific Connector from the Console, it might have affected the other un-edited severity filters for that Connector. Because of this, the agent-severity for all events coming from that Connector was set to "very-high."</p> <p>This issue is fixed, but leaves already-affected severity filters misconfigured. To fix them, manually set the "severity filters" condition to false if you do not intend to use Connector Severity Filters, or modify them to be correct if you do use them.</p> <p>After you install this service pack, you can identify misconfigured filters as follows: go to https://localhost:8443/arcSight/web/manage.jsp > AgentStateTracker, and look at the AgentsFilters table to identify misconfigured Connectors (localhost or IP address, depending on how you registered your Manager). The new Discrepancy column for a Connector states the reason why a Connector Filter is misconfigured. For this issue, it says "This filter condition is set to True." An empty column indicates that the connector severity filter is not misconfigured.</p>
ESM-47359	<p>When a report is created from an active channel as channel report, an error message is displayed:</p> <p>Report Creation Failed.java.lang.NullPointerException</p> <p>This bug has been fixed in ESM 5.0 SP2 and now the report can be generated successfully without error message.</p>
ESM-47205	<p>The ESM feature for Batch update of connectors broke connectors by corrupting the connector configuration files on selected connectors, in ESM 5.0 and 5.0 SP1.</p> <p>This is now fixed.</p>
ESM-47143	<p>The resource tree in the Navigator window collapsed when applying changes to resources.</p>

ArcSight Database

Issue	Description
ESM-47982	<p>If you chose a directory other than ORACLE_HOME for the Data File directory, the installer removed all files in that directory.</p> <p>Now no files are removed.</p>
ESM-47720	<p>For AIX, if the following message is printed in the agent.log file: "Unable to create archive file" apply the following workaround by entering these commands on the command line:</p> <pre>prompt > arcdbutil sql SQL>conn / as sysdba SQL>ALTER SYSTEM set filesystemio_options=ASYNCH scope=spfile; SQL>shutdown immediate; SQL>startup SQL> show parameter filesystemio_options //output should print ASYNCH as the value SQL>exit</pre>
ESM-47611	<p>The database template file, XXLarge.dbt, for Oracle 11g set compatibility incorrectly to 10.2.0.1.0 instead of 11.2.0.1.0.</p> <p>This is now fixed.</p>

Issue	Description
ESM-47479	<p>The command line options for import_system_tables have changed to accommodate the file path of the export dumpfile.</p> <p>Below is the usage detail for import_system_tables command line option.</p> <pre>arcsight import_system_tables <export_username> <import_username> <password> <db_instance> <dump_file_path> <dump_file_name></pre>
ESM-47412	<p>The character set AL32UTF8 caused the Manager solutions package to fail to upgrade.</p> <p>This problem no longer occurs.</p>
ESM-46824	<p>In 11g new installs, the arc_event_data and arc_event_index tablespaces are set to autoextend until maxsize value.</p> <p>Similarly, in case of upgrades any new data files added for arc_event_data and arc_event_index using "arcsight database xts" will also have the autoextend on until the maxsize value.</p>
ESM-35893 TTP#56544	<p>The commands "threaddump" and "dbsessions" are frequently used during manager and/or database troubleshooting. This release introduces the "dbsession" command that is complementary to the 'arcsight threaddump' command and introduces a script to more easily gather dbsessions. It can be implemented through a CRON job or Windows Task Scheduler to control timing and appends output to a file.</p>

ArcSight Manager

Issue	Description
ESM-47651	<p>When you configured a Filter-Out condition for a specific connector from the console, it affected all other Severity-Filters for that connector. The configured filter-out was effective, but the condition of all severity-filters was set to "True." This set the agent-severity for all Events coming from that connector to "very-high." This is now fixed.</p>
ESM-47625	<p>During case export, the Creation Time was changed to the time of the export. The creation time is no longer reset.</p>
ESM-47597	<p>When assets were deleted, the information was still held in cache such that if you attempted to import the deleted assets again, it would cause a conflict error. Now deleted assets are removed from the cache and re-importing works without error.</p>
ESM-47526	<p>Asset creation for assets with the same hostnames but different domain names were resolved as duplicates. As a result, while importing assets using the Network Import Tool or Asset Import Connector, all assets would not get created. The default behavior is now to check the domain and hostname parts to create an asset.</p>
ESM-47507	<p>In ESM v5.0 SP1 patch 2, you could not run report ' Cache History by Connector.' This report now runs correctly.</p>
ESM-47482	<p>After Actors were imported into ESM using the Model Import Connector, when the Manager restarted, it stopped processing events.</p> <p>Now the sequence for Manager startup has been improved to avoid deadlock conditions while loading Actors.</p>
ESM-47471	<p>The name of the customer was incorrectly set for ArcSight Internal Events if the customer had rules or Data Monitors that aggregate on only a few customer related fields rather than aggregating on all customer related fields.</p>

Issue	Description
ESM-47363	If the customer name contained the special character '&' in the OI (organization group(s)) the group did not get processed when translated to a URI. When this happened, it prevented any Actor from getting created in the List.
ESM-47152	If you had a case channel being sorted on an integer field, for example Display ID, if you created a new case, you got an error similar to the following: ArcSightRuntimeException: java.lang.Integer cannot be cast to java.lang.Long. Creating a new case in this situation no longer causes this error.
ESM-47144	When you selected the geographic view from events in an active channel, both Longitude and Latitude information were shown as 0. This bug is fixed in ESM 5.0 SP2 and now the geographic view can show correct information.
ESM-47102	When you created a resource link by linking the group, if the individual resource was deleted, the Console did not display a prompt asking if you want to delete the resource or remove it from the group. It only asked to confirm the delete. This led to unwanted removal of any other instances of the resource.
ESM-46970	The schema validator did not check for the arc_trend_runs table.
ESM-46963	If you tried to modify the GroupIn Asset Condition in CCE, the "Apply" button only worked the first time. Subsequent use of Apply did not have any affect This is now fixed.
ESM-46951	When the property report.csv.header=true was defined in the server.properties file and the report was run in .csv output format, you saw an error similar to the following: [timestamp] com.arcsight.server.reports.ReportException: Failed to archive report [URI], cause by null
ESM-46717	During ESM Manager installation on Windows 2008 R2, ESM Manager could not be set up as a service and the Manager would not start. This is now fixed.
ESM-46301	If you configured a custom banner, it popped up multiple times while starting the Console. Now it only displays the banner once.
ESM-46097	The execute command action was not working . This issue is fixed and for this option to work properly user must specify the absolute path to command.
ESM-45793	The size limit of strings in the Active List is now enforced at 1000 characters.
ESM-45705	The Archive Report Name was set incorrectly when reports were scheduled at same time. This issue is now fixed.
ESM-45693	Sort order was incorrect in report output.
ESM-41492 TTP#68976	If the severity field was set in a Rules Action Tab and the correlation event was forwarded to an SNMP trap sender or Active Channel, the new severity value didn't get reflected. The severity value was overwritten by the priority value.

ArcSight Web

Issue	Description
ESM-47730	It was possible to log in to ArcSight Web using a blank password, if you have Novell eDirectory LDAP service, configured ESM to use password authentication, and select Simple LDAP bind for the authentication Method.

Issue	Description
ESM-46876	The URL generated by the Launch Browser feature of the Dashboard Custom Layout would fail to establish a session after a certain period of time.
ESM-45669	Tags for Dashboard elements in the Web Console were not displayed correctly if there was limited screen space. Now arrow keys are provided and all elements are displayed as expected.

General

Issue	Description
ESM-47718	<p>In some cases, when installing the database on Linux 5.5, there is a JDBC connection failure (timeout). If this occurs, modify the file <code>dbsetup.sh</code> located in the <code>db/bin/scripts/</code> folder. Change the line:</p> <pre>ARCSIGHT_JVM_OPTIONS="-Xmx256m"</pre> <p>to</p> <pre>ARCSIGHT_JVM_OPTIONS="-Xmx256m -Djava.security.egd=file:/dev/./urandom -Dsecurerandom.source=file:/dev/./urandom"</pre> <p>Restart the oracle installation.</p>
ESM-47410	The Install Guide previously showed a screen for the Web server installation with a previous version number. It has been removed from the Install Guide.
ESM-47209	<p>The Send Logs feature still functions, however it no longer automatically uploads logs to ArcSight support.</p> <p>Send Logs creates a compressed file that you can manually email to ArcSight Support.</p>
ESM-46147	As part of ESM v5.0 SP1 the product life cycle document and the DB installer are back in sync and RHEL v4 will not generate any error messages when attempting to install. RHEL v4 EOL took affect in March 2011 and the product will now notify the customer that the platform is no longer supported.

Installation and Upgrade

Issue	Description
ESM-47447	The error, "Error enabling FIPS mode..." occurred when installing ESM Manager 4.5 SP3 with FIPS mode on Solaris 10. This was caused by failure to install correct libraries. Now the installation works correctly in FIPS mode with the correct libraries installed.

Issue	Description
ESM-46685	<p>During an upgrade from Oracle 10g to 11g, you got a TNS Listener error and could not proceed with the upgrade.</p> <p>On Windows, prior to upgrading, remove the ORACLE_HOME environment variable, then reboot your server for the changes to take effect.</p> <p>If you have already upgraded and you are getting the TNS Listener error during post-upgrade tasks, do the following:</p> <ol style="list-style-type: none"> 1. Go to Control panel > System > Advanced > Environment variable. 2. Change the ORACLE_HOME variable to point to the new Oracle 11g home. 3. Click OK to save. 4. Click OK on the TNS Listener error pop-up. Then click Next. <p>This should allow you to proceed with post-upgrade tasks and also complete your upgrade.</p>
ESM-41605 TTP#69383	<p>During ESM configuration, the installer sometime used incorrect terminology for Windows. For example, Next or Previous. Now such choices are correctly yes, no, cancel, and/or back.</p>
ESM-41074 TTP#67951	<p>On Macintosh platform only: If your JRE was updated, you will see the following error in console.log file when you try to log into the Console: IOException: Keystore was tampered with or password was incorrect. Also, when you configure the Console you'll see the following message: Problem checking for the demo CA certificate in '/Users/arc sight/45sp3/Console/current/config/keystore.te mpca'</p> <p>This happens because the Mac OS update changed the password for the cacerts file in the system's JRE. Workaround: Before you start the Console, change the default password for the cacerts file by setting it to the following in the client.properties file (create the file if it does not exist) in the Console's \current\config folder by adding: ssl.truststore.password=changeme</p>

Localization

Issue	Description
ESM-47342	AD Model Import Connector could not import users (Actors) with Japanese characters.
ESM-37264 TTP#60312	Destination start and end times did not save in the Console on Windows XP when localization was set to Italian. This is now fixed.

Open Issues in v5.0 SP2

Analytics

Issue	Description
ESM-47929	<p>Some solutions, system, or customer reports that executed correctly on Oracle 10g, may fail on Oracle 11g with the error "Unable to execute query: ORA-00979: not a GROUP BY expression."</p> <p>The workaround is to:</p> <ol style="list-style-type: none"> 1. Log in to Oracle as "sysdba" 2. Run the following SQL: <pre>alter system set "_optimizer_distinct_agg_transform"=false scope=both;</pre> 3. Reboot Oracle to make the change effective to all sessions.

ArcSight Console

Issue	Description
ESM-48324	<p>On MAC on attempt to follow the link to see a statement of Arcsight third-party copyright notices and license terms from Help --> About the page returns an error.</p> <p>The solution for this issue is to remove extra characters in the end of the URL. The correct URL is http://www.arcsight.com/collateral/copyright_notice/ThirdParty_Copyright_Notices_and_License_Terms.pdf</p>
ESM-48275	<p>On the Console after viewing an ancillary file in the web viewer, if you click on an external URL then you cannot close the web viewer.</p>
ESM-47292	<p>Using the Execute Command Rule Action with parameters of type Date/Time requires that the variable name be within double quotes.</p> <p>For example, to use, \$endTime as a parameter to a command to be executed on rule action, enter the parameter as "\$endTime".</p>

ArcSight Database

Issue	Description
ESM-48332	<p>After having upgraded your Oracle instance, when you start the partition archiver, you might see a "Test Export Failed!" error message in the agent.out.wrapper.log file. If so, check the ' /etc/environment' file and make corrections in it for the updates you did during the upgrade.</p>
ESM-47968	<p>For Windows versions, even though a domain user is a member of the Administrators group, the application launched by the user does not have elevated privileges by default. This is a Windows UAC 'feature.'</p> <p>In this particular case,</p> <ul style="list-style-type: none"> - User logs on as a domain user, who belongs to the Administrator group. - User runs agentsetup from a regular dos shell (for example). - This application does NOT have elevated privileges. - Agentsetup tries to install the partition archiver (PA) as a service and it fails because the application does not have elevated privileges. <p>To remedy this, run agentsetup as Administrator, so it will have elevated privileges:</p> <ul style="list-style-type: none"> - Start cmd.exe as Administrator. To do this, Start > Type cmd.exe in the search box > Right-click on cmd.exe > Run As Administrator. - run agentsetup. - Provide all the required information. - When agentsetup asks for the user-name and password for the user under whose id the PA service will run, specify a local OR domain user, as long as the user belongs to the ORA_DBA group. - This will install PA to run as the specified user.

ArcSight Manager

Issue	Description
ESM-48315	<p>Sometimes, on a 32 bit platform, the Manager process restarts with this error message:</p> <p>Native memory allocation (malloc) failed to allocate 32776 bytes for Chunk::new</p> <p>The workaround is to add the following to server.wrapper.conf:</p> <p>wrapper.java.additional.12=-XX:-DoEscapeAnalysis</p>
ESM-46291	<p>When configuring the Manager with a separate process for a large report (by adding report.canarchiveinseparateprocess=true to the server.properties file), the report would fail with a java.io.FileNotFoundException. This error no longer occurs.</p>
ESM-33431 TTP#51053	<p>In some older versions of ESM with Oracle 10G, 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"> 1 Set the following property in the <ARCSIGHT_HOME>/config/server.properties file: server.date.correction.recoverFromBCDate=true 2 Restart the Manager. <p>Should this issue occur, notify ArcSight Customer Support.</p>

Installation and Upgrade

Issue	Description
ESM-48280	<p>ArcSight Web Installation fails in FIPS suite B mode.</p> <p>The workaround is:</p> <ol style="list-style-type: none"> 1. Update the value of 'TLS_RSA_WITH_AES_128_CBC_SHA' as it appears in the parameter ssl.cipher.suites in Web config/client.defaults.properties to be the same as the value of servletcontainer.jetty311.socket.https.ciphersuites in config/server.properties of Manager. <p>For example,</p> <p>The original setting in the web is:</p> <pre>ssl.cipher.suites=TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA</pre> <p>The first value is updated with 'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA', so the parm setting is now as:</p> <pre>ssl.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA</pre> <ol style="list-style-type: none"> 2. Rerun the webserversetup.

Localization

Issue	Description
ESM-48065	<p>In a Japanese environment, if your upgrade fails with "RedudentNameResourceException," remove the alias for the data monitor '/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Connector Status' and then proceed with upgrade.</p> <p>The resourceid for the above data monitor is 'CYUm2EvMAABCAg2woyOTK3w=='</p>

Issues Remaining Open From v5.0 SP1

The following issues are carried forward from previous ESM releases and remain open in v5.0 SP2. Review these issues to avoid difficulties.

Analytics

Issue	Description
ESM-46828	<p>The rules engine recovery process does not properly restore the state of rules with an aggregation threshold greater than 1. For example, a rule looks for 10 events matching certain conditions with an OnFirstThreshold trigger. If five matching events are received prior to a manager restart, and five more are received after the restart, the threshold trigger will not fire because the partial aggregation state was not reset correctly during recovery.</p> <p>The problem does not affect join rules. For a rule with multiple event aliases, if a subset of the event aliases are matched prior to restart and the remaining ones are matched afterward, the rule will fire correctly.</p> <p>There is no known workaround.</p>
ESM-40795 TTP#67303	<p>Custom cell names created in ArcSight ESM v4.x are not validated for name conflicts with global and local variable names in v5.0 SP1. If you experience issues due to name conflicts, change your custom cell names.</p>
ESM-40748 TTP#67210	<p>After initially importing 50k Actors, you may experience sluggish performance in queries and channels. Performance improves after subsequent statistics collection.</p>
ESM-40529 TTP#66801	<p>After installing IdentityView 1.1, some previously valid ESM resources show as invalid resources.</p> <p>Workaround: Edit the filter called Built In Identities on IDM System and remove the setAction local variable.</p>
ESM-40449 TTP#66622	<p>If you want to export events from the case details channel and there are archived events, the archived events will not be included in the export.</p>
ESM-39856 TTP#65477	<p>If you use the embedded browser in Windows to view a report, the report may not appear until you resize the panel.</p> <p>Workaround: If this keeps happening, resize the panel before running a report. You may want to try several re-sizings to get the desired results.</p>
ESM-39632 TTP#64943	<p>Copying and pasting are not supported for conditions with variables. For example, if you create a filter for an active channel and used the Common Conditions Editor to add condition statements, copying and pasting into another editor (for example, a Rule editor) may result in an error.</p> <p>Workaround: Manually re-enter the conditions.</p>

Issue	Description
ESM-39593 TTP#64837	<p>There is a performance issue when running channels or queries with conditions on actor global variables.</p> <p>Workaround: If you are experiencing this problem, then generate session list statistics as follows:</p> <p>Run the following three commands in <ARCSIGHT_HOME>\bin on your database machine:</p> <pre>./arcdbutil sql username/password @../utilities/database/oracle/common/sql/runSessionListStats.sql exec runSessionStats</pre> <p>The runSessionStats command gathers statistics on all session list tables and gathers both global- and partition-level statistics. You should see an improvement in performance. Note that the scripts may run for a long time if the session lists have a lot of data.</p>
ESM-39554 TTP#64742	<p>When querying events with conditions on actor fields, SQL queries may run slow especially in the following cases:</p> <ul style="list-style-type: none">- List conditions are used.- Conditions on event fields are missing. <p>In some cases, queries may even time out and not produce results.</p>
ESM-39044 TTP#63709	<p>IP addresses are not imported correctly into ArcSight Interactive Discovery (AID) from a CSV file. This is because the IP addresses are getting imported as floating point numbers and are therefore truncated. Importing from an Excel spreadsheet does not have this issue; however, the size limit of an XLS file prevents importing large data sets.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Create the CSV with the desired columns, for example: Name, Source Address, Destination Address.2. Create a schema.ini file that has the following definitions for the CSV file: <pre>[yourfile.csv] ColNameHeader=True Format=CSVDelimited Col1="Name" Char Width 255 Col2="Source Address" Char Width 255 Col3="Destination Address" Char Width 255</pre> <p>This format instructs the driver that the IP addresses are to be imported as strings and not as numbers. The general format is as follows:</p> <pre>[yourfile.csv] ColNameHeader=True Format=CSVDelimited Col1=A DateTime Col2=B Text Width 100 Col3=Col3=C Text Width 100 Col4=D Long Col5=E Double</pre> <p>For more information about the schema.ini file, perform an Internet search.</p>

Issue	Description
ESM-38902 TTP#63460	<p>Importing or exporting domain fields show these fields to be Unknown Fields in the rule editor.</p> <p>Workaround: In the export and import, make sure to include the domain field set to which the domain fields belong.</p>
ESM-38702 TTP#63091	<p>When a group is added to a package, all its contents are automatically included. For top-level groups, as in the case of All Actors, this can include everything under this group. You can implicitly exclude an added group through the Only If Referenced option. This behavior applies to resources in general. If you create a package with a top-level group like All Actors, removing this package also removes all the resources of this top-level group's type.</p> <p>Workaround: To prevent accidental removal of a top-level group, as in the case of All Actors, create a group under it and add a number of actors to this group. Then add this group to a package. If you remove this package, you are only removing the associated groups and resources in that package.</p>
ESM-38079 TTP#62044	<p>If you rename a resource that has dependent resources, don't re-use the deleted name when creating another resource of the same type because the dependent resources may refer to the new resource with the old name.</p>
ESM-37810 TTP#61524	<p>For scheduled reports, when the "Run as" User's read and write privileges are taken away, the scheduled report is generated by the User who created the schedule (and not by the "Run as" User). If the "Run as" User has "read" privilege only, then the report is not generated.</p>
ESM-36755 TTP#58617	<p>If you export an active list into a comma-separated values file and re-import from the same CSV file, the data is corrupted.</p>
ESM-35381 TTP#55314	<p>Variable names that contain hyphens (-) do not work properly when included on the right side of a comparison in a condition statement. For example, consider a rule with a condition that compares the JME argument sqrt(4) to a variable named abc-cde, where the value of abc-cde is:</p> <p>add (2.0,3.0)</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 hyphens (-) in variable names. Underscores (_) are acceptable in variable names, and upper and lower case letters only are best.</p>
ESM-35070 TTP#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>
ESM-34872 TTP#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>
ESM-34531 TTP#53435	<p>When you set the Schedule Frequency for a report, the Next Run Time field is displayed incorrectly in the Editor. Even though the time is displayed incorrectly, the report runs at the time specified in the editor.</p>

Issue	Description
ESM-33525 TTP#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 style="padding-left: 40px;">The query run failed because of the following reason:</p> <p style="padding-left: 80px;">com.arcsight.common.ArcSightException: com.arcsight.common.introspection.queryable.QueryableFetchException:</p> <p style="padding-left: 40px;">Encountered persistence problem while fetching data: Unable to execute query: ORA-00979: not a GROUP BY expression</p> <p style="padding-left: 40px;">Conditional variables in a SELECT statement with an aggregated field causes an Oracle exception (not a GROUP BY expression)</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1 Remove the ORDER BY fields in the Query resource. 2 Use the sort options provided by the Query Viewer or the Report.
ESM-29633 TTP#40230	<p>Sometimes after changing a trend's description, another trend depending on this trend may become invalid. This affects all versions, all users, all ESM platforms.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making a minor change on the trend and then saving it. This will force the re-validation of the trend and usually re-enable the trend. For example, you could toggle the trend's enabled state off and then back on.</p>
ESM-29348 TTP#39407	<p>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).</p>
ESM-26488 TTP#33835	<p>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.</p> <p>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.</p>

ArcSight Console

Issue	Description
ESM-47414	<p>A quick logger search using One-Time Password (OTP) in the embedded browser fails after a Logger session has been inactive for 'Logger Session Inactivity Timeout,' for which the default is 15 minutes.</p> <p>The workaround is to use the external browser to see results.</p>

Issue	Description
ESM-46633	The Help window for Rules is inactive. This is seen when you are defining a Set Event Field action. Click cancel or OK in the Set Event Field window. This will allow you to see the help information. After reading the help, you can go back to entering settings in Set Event Field.
ESM-46629	<p>On the Mac OS X with Safari as the default browser, the context Console Help is not displayed. Instead, the browser displays a blank Help page. This is a known Safari behavior, which does not accept more than one # character in the URL. The URLs to the Help pages contain more than one # symbol.</p> <p>Workarounds:</p> <p>Use either Firefox instead of Safari as the default browser. If you still want to use Safari, after the Help page loads, use the Contents tab to select the desired topic or use the Search tab to search for specific topics.</p>
ESM-46594	The Category Device Type field is not supported during event categorization from Console. You should not set the Category Device field.
ESM-46226	<p>The GetGroupOfAsset variable function does not return results in SQL mode (in conditions for reports, query viewers, pattern discovery, active channels). This problem is seen in all ESM platforms.</p> <p>There is no workaround at this time.</p>
ESM-46065	<p>The embedded browser is not supported in Solaris.</p> <p>Workaround: Use an external web browser to navigate help pages. Go to Preferences > Global Options and check "Launch Help in external web browser"</p>
ESM-41344 TTP#68478	<p>When viewing image dashboards in an external browser, if you keep the dashboard running, you will get an error saying that a script on the page is causing the browser to run slowly and if it continues to run, your computer may become unresponsive. This error appears after every few hours while the image dashboard is running.</p> <p>This is a known issue. Click No to dismiss the message. You may also refresh the page.</p>
ESM-41247 TTP#68262	<p>If you set "NSPAuth" as Password type and run TRM commands in the external browser, you will be redirected to the Login page.</p> <p>Workaround: Set NSPAuth to Text type if you want to use the external browser for TRM commands. One issue with this workaround is that the authentication token would appear as clear text in your browser URL parameters.</p>
ESM-41190 TTP#68141	If you set "LoggerPassword" as Password type and run Logger commands in the external browser, you will see an "Authorization Request" message in your browser.
ESM-41116 TTP#68018	After creating a statistics data monitor, adding it to the dashboard, and switching to custom view mode, the dashboard is not launched. This was seen using the external IE browser on a 64-bit Windows platform. This is because Adobe Flash Player is required but is not supported on IE in 64-bit systems.
ESM-41019 TTP#67856	<p>If Manager is configured with the "Password and SSL Authentication" and you have client-side authentication set up, you will get an error when accessing the ESM documentation using both the embedded browser in the Console as well as the external browser.</p> <p>Workaround: Generate a key pair for browsers and import the certificate into Manager's truststore; or copy the Console's key into the browser's keystore. See the ArcSight ESM Administrator's Guide for details on how to do this.</p>
ESM-40999 TTP#67820	There is a performance issue when loading active channels. The channel starts to load but displays Loading Event ID for a few minutes before completely loading.

Issue	Description
ESM-40985 TTP#67798	On Solaris only: From the Console, support for web browser functionalities is limited to only viewing the online help in the external browser.
ESM-40935 TTP#67689	On a Windows Vista 64-bit system, charts cannot be viewed in custom view dashboards when using IE as external browser. Workaround: Use the 32-bit browser, such as 32-bit version of IE or Mozilla Firefox, and also download Adobe Flash Player.
ESM-40917 TTP#67652	If you are deleting a large number of actors through the Console, the Console may be temporarily unusable. ESM Manager continues processing in the background and updates the database with your changes. The Console becomes available again but deletion from the database may take longer. In some cases, for instance if the server is terminated or encounters an error, not all deletions may be completed, leaving the actors data in an inconsistent state. Contact ArcSight support for assistance in detecting and cleaning up this condition if you suspect it has occurred.
ESM-40782 TTP#67265	The Console's embedded browser is not supported on Red Hat Linux 5. Workaround: Use the external browser instead.
ESM-40739 TTP#67195	After accepting the certificate from ESM Manager during the login process, that is, the first time this installation of the Console is connecting to the Manager, restart the Console for custom view dashboards to work properly.
ESM-40587 TTP#66906	Correlation events may occur before the base event that triggered the correlation event in channels sorted by time. This happens if the event end time for the correlation event is the same as that for the base event. Workaround: Add a sort column in the channel to sort events, first by end time, and second by type of event. Base event type is 0 and correlation event type is 1.
ESM-40514 TTP#66766	On a 64-bit Macintosh, displaying online help in the embedded browser is not supported. Workaround: Use an external browser instead.
ESM-40506 TTP#66753	On the Macintosh platform, setting Safari as the preferred external browser using the Console's Preference menu (Edit>Preferences>Program) will result in the wrong URL. Workaround: Change the setting from the Console's Preference menu (Edit > Preferences > Program > Preferred Web Browser > External Browser) to open. Next, make sure Safari is the default browser in your Mac OS (Safari > Preference > General > Default) web browser.
ESM-40302 TTP#66337	The server.log showed an exception when a custom view dashboard was launched in FIPS mode. Custom view dashboards are not supported in FIPS mode.
ESM-39980 TTP#65708	The Console can become unresponsive if you are trying to access other resources while building category models with a large number of actors.
ESM-39963 TTP#65671	If an active channel uses a filter that applies conditions to a list data type field, then multiple rows will be seen in the active channel for the same event or resource. Workaround: There is no workaround. This is a display issue. You may ignore the duplicate rows.

Issue	Description
ESM-39829 TTP#65421	<p>When there are category models in ESM, deleting actors will require these category models to be re-built. Each rebuild may take seconds. In case of thousands of actors are deleted, the whole deletion period may last for hours because actor deletion launches a category model rebuild.</p> <p>There is no workaround so far in current implementation. Our current implementation sends deletion requests one resource a time.</p>
ESM-39331 TTP#64251	<p>If you create an actor channel, add any new fields to the field set being used by the channel instead of directly to the channel.</p>
ESM-39322 TTP#64233	<p>When viewing a Category Model, if the user is a non-admin user, a NullPointerException will be thrown by the Arcsight Console, even if the user has been given read and write rights on all the actors and the Actor Base field set.</p> <p>Workaround: View the Category Model as an admin user.</p>
ESM-39101 TTP#63834	<p>In Suite B mode, the custom view dashboard cannot be launched.</p> <p>Workaround: Use an external web browser. Go to Preferences > Programs and deselect "Use the web browser embedded in ArcSight Console"</p>
ESM-38961 TTP#63568	<p>For image view mode, when a background file is uploaded, the Console does not provide an option for a location. The file automatically goes into the user's personal folder.</p> <p>Workaround: After the upload, the user can move the file to a preferred folder.</p>
ESM-38415 TTP#62565	<p>In an active channel, you cannot add global variables to the channel through the right-click option, Add Column. Only global variables already added to the current field set will be displayed.</p> <p>Workaround: Add the global variables you want for the channel to a field set, then choose that field set for your channel.</p>
ESM-38014 TTP#61931	<p>When a filter is moved from one group to another and data monitors that depend on that filter is packaged, exported, and re-imported on a different ESM installation, the data monitors may have missing filter attribute values.</p> <p>Workaround: Manually set the filter for these data monitors that are identified by the broken resource icon.</p>
ESM-37868 TTP#61659	<p>When a user modifies a case while a case channel is open and an inline filter is applied, no data appears. To successfully display available data, the case channel has to be refreshed.</p>
ESM-37344 TTP#60500	<p>On a Manager where a large number of cases reside in a single group, the user can't pick a case for "Add to Existing Case" rule action in the Rule editor. The reason is that the resource selector only shows leaf nodes when there are less than 1000 cases in a group. The scope of this bug actually goes beyond cases. It happens for all resources in ESM.</p> <p>Workaround: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.</p>
ESM-37079 TTP#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>
ESM-36055 TTP#57050	<p>In the Query Editor, if you have read permission to a query but not to the global variables that are being used in the query, the resulting display will be incomplete. None of the global variable-related fields will be displayed. Also, you will not get an error saying that you are not able to view some resources in the query due to lack of sufficient permissions.</p>

Issue	Description
ESM-35998 TTP#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.
ESM-35853 TTP#56430	The Aggregation tab is not working for the Report table template. Workaround: For the Aggregation tab to become active, a user must not only apply a function to a column but also select a grouping column.
ESM-35830 TTP#56367	ESM v5.0 is compatible with TRM v4.6. However, certain commands that were introduced in a later version of TRM are available when you use the integration tool from TRM v4.7 to connect to TRM v4.6. If you try to execute such commands, you will receive a java.lang.NullPointerException exception. One such command introduced in TRM v4.7 is Generate N/W detail as CEF. Workaround: It is recommended that you upgrade to TRM v4.7 or higher. If you upgrade to TRM v5.0, you will be able to use the integration commands feature.
ESM-35465 TTP#55476	If you open 10 channels and view them, then delete these 10 channels from the resource tree, you will not be able to open any more channels. You will see the following error: "Unable to create communication mode with server: The maximum number of open event channels (10) has been exceeded. Please close one or more individual event channels to continue." Workaround: Restart the Console.
ESM-34830 TTP#53912	On the ESM Console, the Connector configuration settings do not support decimals for the "Limit event processing rate" option (only integer settings are supported for this release), even though decimals are supported for this option on the Connector. Note: Select a Connector in the Navigator, right-click and choose "Configure" to bring up the configuration for that connector in the Inspector panel. Select the "Default" tab and then "Content" subtab. The "Limit event processing rate" option is under "Processing." Only integer settings are supported for this option on the Console.
ESM-33453 TTP#51094	On Unix systems: The drag-and-drop feature does not work on the Console. Workaround: Use the cut-and-paste feature instead.
ESM-33440 TTP#51072	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-33360 TTP#50968	If you delete an escalation-level notification resource, you will receive the error Group does not exist in the console.log file. This error is incorrect and can be ignored.
ESM-32705 TTP#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.
ESM-32489 TTP#49024	Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.
ESM-31127 TTP#45403	An embedded browser in the Console is not supported on the Linux 64-bit platform. Workaround: Use an external browser instead. You can set up the Console to use the external browser during installation.
ESM-30791 TTP#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.

Issue	Description
ESM-28890 TTP#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>
ESM-27970 TTP#36148	<p>To search for Resource IDs that begin with non-alphanumeric characters (such as the Resource IDs for Trends and Queries), enclose the ID in double quotes. For example, to search for</p> <pre>^VVsOXg4BABCAIEuBhILMyg==</pre> <p>Enter</p> <pre>"^VVsOXg4BABCAIEuBhILMyg=="</pre> <p>in the query text field.</p>

ArcSight Database

Issue	Description
ESM-46556	<p>During the Oracle database installation, at the step when you are creating a database instance, the wizard does not warn you if you use an instance name with a space, for example:</p> <pre>arcsight db</pre> <p>Oracle does not allow spaces, and therefore the instance creation will fail. Do not use spaces for database instance names.</p>
ESM-46503	<p>Due to an issue with Oracle 11g, documented in Oracle Metalink article 1173167.1, when installing Oracle 11g on Unix platforms, if the DISPLAY variable points to an invalid Xserver, the Oracle 11g installation will fail with an error like "...Xlib: connection to ":0.0" refused by server Xlib: No protocol specified" or "Exception in thread "main" java.lang.NoClassDefFoundError at java.lang.Class.forName0(Native Method)" in the <ARCSIGHT_DB_HOME>/logs/database.installation.log.</p> <p>Workaround: Unset the DISPLAY variable before starting the Oracle 11g installation.</p>
ESM-46330	<p>The command line function to archive, deactivate, or reactivate partitions does not work if non-default values of archive, retention, and reserve period days are used.</p> <p>Workaround: Use the Console to perform the task.</p>
ESM-39206 TTP#64037	<p>When querying events with conditions on Actor fields, SQL queries may run slow especially in the following cases:</p> <ul style="list-style-type: none"> - List conditions are used. - Conditions on event fields are missing. <p>In some cases, queries may even time out and not produce results.</p>
ESM-35884 TTP#56521	<p>If you start the Partition Archiver as a service, the PATH does not get set correctly for the Oracle user if you use /usr/bin/bash.</p> <p>Workaround:</p> <ul style="list-style-type: none"> - While logged in as the oracle user, run the Partition Archiver as a standalone application with "arcsight agents" command; or - Switch to /bin/sh which is the default Oracle shell in /etc/passwd.

Issue	Description
ESM-35620 TTP#55853	<p>The ArcSight Database installer does not include error checking or validation against Oracle-supported schema user naming conventions. If the user names specified contain anything other than alphanumeric characters, the ArcSight Database installer will prevent creation or re-creation of the schema and will display the following error code:</p> <p>error ORA-00921: unexpected end of sql command</p> <p>Workaround: For ArcSight Database install and schema setup, 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>
ESM-34568 TTP#53484	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <p>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</p> <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 ARC_TEMP table.</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" in Appendix B of the ArcSight ESM Administrator's Guide.</p>

ArcSight Manager

Issue	Description
ESM-46572	<p>During an actor import using the Model Import Connector, some archive files may be saved with the file name extension, .bad. If those files are subsequently manually imported, in some cases the result may be incomplete actor information loaded into the database. This does not affect any actors that were successfully imported from the Model Import Connector. There is no known workaround at this time.</p>
ESM-46045	<p>Occasionally you will see inconsistent behavior with domain field population in the active channel and Event Inspector panel after restarting the ArcSight Manager. Domain fields do not get populated even though correct domain is picked.</p>
ESM-41331 TTP#68451	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: Manually mark assets that are known to be invalid as invalid.</p>
ESM-41272 TTP#68310	<p>Asset Aging tasks will not proceed if you have disabled assets in the system.</p> <p>Workaround:</p> <p>Use one of two options:</p> <ul style="list-style-type: none"> - Fix the invalid assets, or - Ignore the invalid assets by adding the following to server.properties: asset.aging.excluded.groups.uris=/All Assets/System Disabled/Disabled Assets
ESM-41215 TTP#68187	<p>On SUSE 11, ESM Manager does not start automatically at system startup even if this option was selected during installation.</p> <p>Workaround: Start Manager manually.</p>
ESM-41208 TTP#68173	<p>If ESM Manager is started as a service on a Windows 2003 32-bit machine, the service cannot be started and an error message may be displayed, even though the ESM Manager is being started normally in the background. Confirm successful Manager startup by searching the Manager's <ARCSIGHT_HOME>/logs/default/server.std.log file for the word "Ready."</p>

Issue	Description
ESM-41168 TTP#68098	Uninstalling and then re-installing the global variable package causes an exception. Global variables are part of the core content, and uninstalling core content is not recommended.
ESM-40889 TTP#67567	The "group:101" audit event may fail to be sent in some cases where there are many role memberships being added or changed for an actor. There will be an error in the server log related to this, which includes the IDs of the affected objects.
ESM-40866 TTP#67496	System zones were modified for this release. So, after importing packages or archives containing assets in zones that were modified those assets will become invalid. Workaround: You need to manually fix the zone for these assets.
ESM-40815 TTP#67348	If a domain field in a filter or rule is deleted, and you re-create the field with the same name, it appears that you can successfully validate the filter or rule. However, the filter does not match or the rule will not fire. Workaround: To prevent this, re-create the domain field, associate it with the same domain field set, then validate the resource.
ESM-37633 TTP#61154	After installing the Manager, you will see an error in the server.log file: [ERROR][default.com.arcsight.config.util.WebProperties][getPassword] com.arcsight.common.ArcSightException: Cannot handle the data which was obfuscated by old scheme This message is harmless and can be safely ignored.
ESM-37488 TTP#60808	When you export a large active list with 10 million entries or more, or export rules that use such active lists, you will see an exception in the server.std.log. Additionally, the Manager runs out of memory and therefore automatically restarts itself. Workaround: You may use the export format instead of the default format while exporting the rule or active list definition using an archive or a package. This will not export the active list data.
ESM-36328 TTP#57661	If the Manager receives a scan for a host that already exists in ESM and belong to a dynamic zone, but giving your new asset a unique domain name, this asset gets created. So, you end up having two assets with the same hostname and dynamic address but different domain names.
ESM-35732 TTP#56123	The Archive tool can sometimes fail to import entries into an active list if the active list cannot be accessed. In such situations, you will not see any errors, but the list does not get populated. Workaround: Import the same package a second time.
ESM-35668 TTP#55969	On Linux only: You may experience high CPU utilization on the ESM Manager. This may be specific to your system/hardware. Workaround: If you are experiencing performance issues, try updating your drivers or reinstalling the Linux operating system.
ESM-33462 TTP#51112	Stages resources are editable from the ESM Console, although these should not be moved or customized. (See ESM Console Navigator > Stages resource tree.) Please keep stages provided as standard content in the given folders and do not move them into another folder. Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created. (For more information, See the "Standard Content" topic in the Console Help.

Issue	Description
ESM-31433 TTP#46276	<p>On Windows only: If you install the Manager as a service, you may see the following error when the Manager starts:</p> <p>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</p> <p>Workaround: This error automatically gets resolved within one week of the Manager startup, during which time the Manager rebuilds the resource search index (done weekly). Optionally, you can manually do a rebuild at any time by running this command from the database bin directory:</p> <pre>arcsight searchindex -a create -m <manager-hostname> -u <admin-user-name> -p <password></pre>
ESM-30670 TTP#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>
ESM-30314 TTP#42730	You cannot move an asset using Auto Zone if the asset is locked.
ESM-30008 TTP#41582	<p>Occasionally, when installing an exported package from a bundle file, you might receive the following error:</p> <p>Install Failed: Resource in broker is newer than modified resource.</p> <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>
ESM-27414 TTP#35166	<p>If you are running the sendlogs wizard and you click Previous or Next, an error message says</p> <p>Error (Null)</p> <p>Workaround: Cancel the wizard and start again.</p>

ArcSight Web

Issue	Description
ESM-35801 TTP#56258	<p>If you create a Case and set the Estimated Resource Time in ArcSight Web, 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>
ESM-35693 TTP#56005	If your session has expired and you click 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.

Issue	Description
ESM-33922 TTP#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, if Use Default is enabled, click to deselect it. Then enter a row limit of 100 or less. 3. Click Apply or OK to save the changes.
ESM-30675 TTP#43702	<p>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:</p> <p>http://www.adobe.com/go/6b3af6c9</p>

Connectors

Issue	Description
ESM-41419 TTP#68697	<p>There is a limitation if a connector needs to send events to multiple ESM Manager destinations with different versions (v4.5 and v5.0, for example). The serialization framework uses the lowest common denominator version (v4.5 in this case) to serialize events prior to sending to them to the ESM Managers. This means only 4.5 events will be sent to both ESM Managers.</p>

Installation and Upgrade

Issue	Description
ESM-46791	<p>The partition archiver does not connect to ESM Manager if configured in Suite B mode. Two workarounds are provided.</p> <p>Workaround for a fresh installation of partition archiver (PA):</p> <ol style="list-style-type: none"> 1. Run "arcsight database pc" as usual to configure PA. 2. Run "arcsight agentsetup" to register this PA. Select the same Suite B mode as the manager. <p>This setup will fail with a pop up error dialog. Close this error dialog and click Cancel to exit the agent setup wizard.</p> <ol style="list-style-type: none"> 3. Edit the <ARCSIGHT_HOME>/user/agent/client.properties file. Set the value of ssl.cipher.suites to be the same as the value of servletcontainer.jetty311.socket.https.ciphersuites in the config/server.properties of Manager. <p>For example, if server.properties has the entry:</p> <pre>servletcontainer.jetty311.socket.https.ciphersuites=TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</pre> <p>Then the user/agent/client.properties should be:</p> <pre>ssl.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</pre> <ol style="list-style-type: none"> 4. Create or edit the <ARCSIGHT_HOME>/user/agent/agent.properties file and add the following line to this file: <pre>fips.enabled=true</pre> <ol style="list-style-type: none"> 5. Run "arcsight agentsetup" again to register PA. <p>Workaround for an upgrade of partition archiver (PA):</p> <ol style="list-style-type: none"> 1. Edit the <ARCSIGHT_HOME>/user/agent/client.properties file. 2. Set the value of ssl.cipher.suites to be the same as the value of servletcontainer.jetty311.socket.https.ciphersuites in config/server.properties of Manager. For example, if server.properties has the entry: <pre>servletcontainer.jetty311.socket.https.ciphersuites=TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</pre> <p>Then the user/agent/client.properties should be:</p> <pre>ssl.cipher.suites=TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</pre>
ESM-46545	<p>After the upgrade, the number of invalid assets listed in the Resource Validation Report may be higher than before the upgrade. This is due to additional validations introduced in 5.0 SP1 release to identify invalid assets.</p>

Issue	Description
ESM-46402	<p>On systems set to French locale, there was a failure during ESM Manager upgrade from 4.5 SP3 Patch 1 to 5.0 GA Patch 1 and to 5.0 SP1. This error was seen at the upgrade step, "Transfer setting from source ArcSight Home."</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Back up the "archive" folder under manager ARCSIGHT_HOME/reports folder of the source Arcsight ESM Manager location. 2. Delete the "archive" folder under manager ARCSIGHT_HOME/reports folder of source Arcsight ESM Manager location. (Required only if you run into an issue.) 3. Resume ESM Manager upgrade by running this command in <ARCSIGHT_HOME>/bin: <pre>arcsight upgrade manager</pre> 4. After a successful ESM Manager upgrade to 5.0 patch1 to 5.0 SP1, copy the "archive" folder from the backup location and paste it under the ESM Manager upgrade location: <pre><ARCSIGHT_HOME>/reports of 5.0 Patch1/5.0 SP1</pre> 5. Start ESM Manger.
ESM-46263	<p>If you try to install oracle 10g and 11g on different drives and upgrade from 10g to 11g, there will be issues with TNS listener startup. Try to install 11g on same drive as 10g.</p>
ESM-41220 TTP#68193	<p>When upgrading packages, the upgrade summary report that provides a list of installed packages may show packages that were not installed after all. You should ignore this. The summary report is in error in this case. Most likely, you did not have those packages prior to the upgrade.</p>
ESM-41148 TTP#68075	<p>During an upgrade to ESM 5.0 GA, autozoning will fail if the number of assets in a zone/group exceeds 1000.</p> <p>Workaround: If this happens, manually run autozoning in batches of 1000 assets or fewer after completing your upgrade. You can do this from the Asset Channel or Asset Resource Tree in the Console.</p>
ESM-40984 TTP#67797	<p>Before uninstalling any ArcSight package, certain tasks must be performed in sequence. Generally, you would remove relationships first before deleting. For example, if the data monitor group is deleted before the data monitor resource, you will encounter a permission error because permissions are tied to groups.</p>
ESM-35653 TTP#55935	<p>ESM Console upgrades from ESM v4.0 SP3, v4.5 SP1, or v4.5 SP2 to ESM v5.0 GA 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. 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.</p>
ESM-35599 TTP#55810	<p>When upgrading the ArcSight Console, you will be prompted to enter the path to the previous Console installation. Be sure to provide the path to the Console's <ARCSIGHT_HOME>/current directory of your previous Console installation.</p> <p>If you do not point to the current directory, you will get an error that the cacerts folder could not be found in this location. Selecting OK will allow you to continue with the upgrade. But, this will cause the certificates to not get transferred and make the upgrade error prone.</p>

Issue	Description
ESM-34891 TTP#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: 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>
ESM-34069 TTP#52690	<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 (for example, 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>
ESM-34011 TTP#52556	<p>You will not be able to do two consecutive upgrades on the same day. For example, upgrading from v4.5 SP1 to v4.5 SP2, then upgrading to v5.0 cannot be done on the same day.</p> <p>Workaround: After doing one upgrade, wait until the execution of the next scheduled Partition Manager job before doing the next upgrade. This allows Partition Manager to create a new partition which allows the system to be recognized as upgraded to an intermediate version. Execution of the Partition Manager scheduled job can be ensured by letting the Manager from the first upgrade run for a day (24 hours). Do the next upgrade after a day.</p>
ESM-33949 TTP#52394	<p>File resources are not handled properly during ESM upgrading. This results in unassigned file resources after the 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.</p> <p>Workaround: You can remove the unassigned .art files after an upgrade, since they are duplicates. The .art files can be safely deleted.</p>
ESM-33766 TTP#51954	<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: Do not use spaces in ESM installation paths. The default install paths (for example, C:/arcsight/Manager) do not include spaces. If you modify the install paths, make sure there are no spaces in the directory names. Use dashes (-) or underscores (_) instead of spaces.</p>
ESM-31766 TTP#47206	<p>During an upgrade to v4.5 SP1, the "SSL Client Only" authentication option is selected by default. If you had set up your v4.0 SP3 Manager to use the "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>
ESM-31728 TTP#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. Ignore this information and continue with the installation/upgrade.</p>

Issue	Description
ESM-31392 TTP#46153	On Solaris: When performing a fresh ESM Manager installation or upgrading ESM, the installation or upgrade does not always complete when solutions packages are installed. 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.

Localization

Issue	Description
ESM-46567	In a localized environment, the Group variable functions, for example GetGroupsOfAsset and FormatGroupsOfAsset, do not return results in active channels.

Pattern Discovery

Issue	Description
ESM-46312	If you create a rule from patterns that use domains, you must aggregate the field, Domain Name. If this field is not aggregated, the rule will not be fired.
ESM-46250	In ESM 5.0 SP1, if a domain field is shared by more than one domain, the event graph is not shown correctly.
ESM-46157	In Profile "Actions" tab, Global Variables are unavailable for "Add to Active List" and "Add to Session List" actions. For example, when "Add to Active List" is selected for "On Pattern Discovered" action, the Active List and the Active List field mappings need to be provided. In the drop-down menu of the field mapping, the Global Variables are disabled.
ESM-35048 TTP#54452	A java.lang.InterruptedExceptioin might be logged in the ESM Manager server.std.out.logs when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.
ESM-20555 TTP#24715	In pattern discovery, if a profile has event fields with the same name as an event annotation stage name, the snapshot will show a null in the resulting event fields. The snapshot will not be forwarded to the event graph.

