

Release Notes

ArcSight Express 4.0

April 10, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

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

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWl .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
04/10/2013	ArcSight Express 4.0	Release Notes

Contents

ArcSight Express 4.0	7
ArcSight Express 4.0 Contents	7
Upgrade Support	7
What's New in ArcSight Express 4.0	8
ArcSight Express Content	8
Connectors	8
Management Console	8
Dashboards in the Management Console	8
Correlation	9
Reporting	9
CORR-Engine Storage	9
Security	9
Environment Updates	9
Geographical Information Update	9
Vulnerability Update	9
Section 508 Compliance	10
Usage Notes	10
Dashboards Containing Geographic Event Graph or Event Graph Data Monitors	10
Dashboard Warnings	10
Browser Support in FIPS with Suite B Mode	10
ArcSight Web and Management Console on Safari Browser	11
Online Help in Internet Explorer with Chrome Frame Plugin	11
Connector Management on Safari	11
Large Trends	11
Windows Unified Event Log Connector	11
Issues Fixed in this Release	11
Analytics	12
ArcSight Console	12
ArcSight Manager	13
ArcSight Web	13
CORR-Engine	13
Installation and Upgrade	14
Management Console	14
Open Issues in this Release	14

Analytics	15
ArcSight Console	17
ArcSight Manager	20
ArcSight Web	22
CORR-Engine	23
Connector Management	23
Connectors	23
General	25
Installation and Upgrade	25
Localization	27
Management Console	27
Pattern Discovery	28

ArcSight Express 4.0

These release notes discuss the following topics.

["ArcSight Express 4.0 Contents" on page 7](#)
["What's New in ArcSight Express 4.0" on page 8](#)
["Environment Updates" on page 9](#)
["Usage Notes" on page 10](#)
["Issues Fixed in this Release" on page 11](#)
["Open Issues in this Release" on page 14](#)

ArcSight Express 4.0 Contents

The files you need to download for this release are:

Table 1 Installed Components

File name	Download Location	Description
If you are upgrading from AE 3.0:		
arcsight-express-4.0.0.xxxx.0.pl	HP SSO website	Upgrade File When you click on the .pl file to download it, its checksum appears at the bottom of the page. After downloading the .pl file, calculate the checksum on your downloaded .pl file and make sure it matches with the checksum provided on the download page.

Upgrade Support

This release supports upgrade from ArcSight Express 3.0 to 4.0 only. Please refer to the Upgrade Guide for details on how to upgrade your ArcSight Express appliance. HP ArcSight highly recommend that you open a ticket with HP ArcSight Customer Support and have your system tables tested **before** you perform the upgrade. See the Upgrade Guide for details and follow the instructions in its "Before You Upgrade" section.

What's New in ArcSight Express 4.0

The following features are new in ArcSight Express 4.0:

ArcSight Express Content

Navigation has been made easier by grouping resources into use cases.

The ArcSight Express content now includes NetFlow Monitoring, Microsoft Windows Monitoring, and Cisco Monitoring. In addition, a trial version of the HP Reputation Security Monitor solution (RepSM) is available. Contact your HP ArcSight sales representative for an evaluation license.

For information about Standard Content for ArcSight Express, refer to the ArcSight ExpressStandard Content Guide. All ArcSight Express documentation is available on Protect 724 at (<https://protect724.arcsight.com>).

Connectors

The ArcSight Express appliance comes pre-configured with two connectors for which most of the set up can be done with the First Boot Wizard:

- Syslog Daemon connector
- Windows Unified Event Log connector

You have the option to install and configure additional connectors on the appliance.

Management Console

New features and improvements include:

- **Connector Management** centrally manages SmartConnectors installed on the ArcSight Express appliance, ArcSight Connector Appliances, or any other system. Use the Connector Management module to manage, upgrade, restore, and adjust connector configurations.
- **Internationalization and localization** support has been added for Japanese, French, and Traditional Chinese.

For more information, see the Management Console User's Guide.

Dashboards in the Management Console

Improvements to Management Console dashboards include:

- Improved dashboard and data monitor layout and navigation
- Improved configuration capabilities
- Dashboard drill-down to other dashboards
- Support for currently-unsupported dashboards
- Support for previously unsupported data monitors (Event Graph, Geographical Event Graph, and Hierarchy Map)

The ArcSight Console has been enhanced to support greater drill-down from data monitors and query viewers to dashboards, reports, active channels, and query viewers.

For more information on Dashboards in the Management Console, see the Management Console User's Guide's "Dashboards" chapter. For the ArcSight Console, see the section "Using Dashboards".

Correlation

- Active List Enhancements include:
 - ◆ SUM, MIN, MAX numeric subtypes
 - ◆ Store data in time segments
- New, lightweight rules that skip multiple event aliases and aggregation, limit actions and auditing for significant performance gains.

Reporting

Reporting has been enhanced to create a report once and distribute it to multiple recipients. You have the option to not send empty reports. Reporting has also been enhanced to define non-ESM users as recipients.

CORR-Engine Storage

CORR-Engine now supports Original Agent and Final Device fields and it can store event annotations in archives.

Refer to the Management Console User's Guide for details.

Security

ArcSight Express now supports the Federal Information Processing Standard (FIPS) 140-2 and Suite B, as described in the Administrator's Guide.

The Management Console now supports SSL Authentication. This is described in the Management Console User's Guide.

Environment Updates

This release contains the following environment updates:

Geographical Information Update

This version of ArcSight Express includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20120501.

Vulnerability Update

This release includes recent vulnerability mappings (February 2013 Context Update) for these devices:

Device	Vulnerability Updates
Short / Sourcefire SEU 815	Faultline, Bugtraq, CVE, Nessus, MSSB
Enterasys Dragon IDS	CVE
Cisco Secure IDS S695	Faultline, Bugtraq, CVE, Nessus

Device	Vulnerability Updates
Juniper / Netscreen IDP update 2232	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
TippingPoint UnityOne DV8414	Faultline, Bugtraq, CVE, MSSB
ISS SiteProtector	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, Nessus, MSSB
Radware DefensePro	CVE

Section 508 Compliance

HP ArcSight recognizes the importance and relevance of accessibility as a product initiative. To that end, HP ArcSight is making and continues to make advances in the area of accessibility in its product lines.

Usage Notes

Keep these tips in mind when using ArcSight Express 4.0.

Dashboards Containing Geographic Event Graph or Event Graph Data Monitors

On Internet Explorer only: In order to load dashboards that contain a Geographic Event Graph or an Event Graph Data Monitor the Google Chrome Frame plugin is required. Workaround: Install the plugin manually from <http://www.google.com/chromeiframe>.

Dashboard Warnings

An open dashboard periodically queries the Manager for new data to update itself. If the dashboard doesn't get a timely response for the request, either because of network latency or slow response from the Manager, the web browser will display the following warning dialog: "Unresponsive Script - A script on this page might be busy or stopped responding" Choose Yes to clear the message and stop the dashboard from updating itself. You need to manually reload the browser as needed. If you choose no, the dashboard will continue trying to update itself, and the warning dialog will continue to pop up.

Browser Support in FIPS with Suite B Mode

If you have installed the product in FIPS with Suite B mode, use the Firefox browser to connect to the Manager.

You cannot use the Internet Explorer browser to connect to the Manager, since Internet Explorer does not support FIPS with Suite B on the following platforms:

Windows XP

Windows 2008

Windows Vista

ArcSight Web and Management Console on Safari Browser

On Macintosh platform only: When accessing ArcSight Web from the Management Console for the very first time, after you accept the Manager's certificate, ArcSight Web opens up in a new tab in the browser instead of opening within the Management Console itself.

Online Help in Internet Explorer with Chrome Frame Plugin

On Internet Explorer only: When using the Management Console, if you click the Help link, the online Help does not open.

To work around this issue:

- 1 Refresh the browser page or click the refresh button. The browser prompts you whether to accept the Manager's certificate.
- 2 Click Yes. The browser will display the Help content.

Connector Management on Safari

On Macintosh platform only: When you open the Connector Management page in the Management Console for the very first time, it opens in a standalone browser instead of being embedded within the Management Console. This happens only when you access it for the very first time, when you have to accept the Manager's certificate.

When you encounter this, click on your browser's back button. It should load in the Connector Management page in embedded mode.

Large Trends

Trends running on ESM with Oracle were often created to provide improved report performance on a subset of columns. This use case is no longer necessary with the improved indexing. As a best practice avoid using trends for creating a subset of columns.

Windows Unified Event Log Connector

If you add the Windows Unified Event Log connector to ArcSight Express, you might get an error.

According to the MicroSoft support site at <http://support.microsoft.com/kb/951581>, LDAP queries are executed more slowly than expected in the AD or LDS/ADAM directory service, and Event ID 1644 may be logged.

If the browser running on Windows takes more than 5 minutes and produces a SocketTimeout error, check the agent.log for the container. If the query time (LDAPUtils info log to performSearch log time stamps) is more than 5 minutes, but returns successful results (as noted in the agent.log), check the Active Directory server for the MS issue (event 1644 in the Directory Service log). As a work-around, you can increase the timeout threshold.

Issues Fixed in this Release

The following issues are fixed in this release of the product.

Analytics

Issue	Description
NGS-1835	<p>During the punitive action period of the EPS License violation, there were two issues related to data monitors:</p> <ol style="list-style-type: none"> 1. For any existing data monitors, when you tried to edit them (right-click and select Edit data monitor), a NullPointerException error dialog was thrown. After the punitive action ended, the data monitor could be edited without any exception. An error message window popped up with NullPointerException and the exception was displayed in the Console stdout 2. When a new data monitor was created, it opened the editor. After you selected a type of data monitor, the editor did not populate the values to be input for the type of data monitor selected and you got an exception in the Console stdout. <p>This issue has now been fixed.</p>
NGS-448	<p>In some cases, a query would run for more than 10 hours (but less than 20 hours) before being canceled. The system now detects these situations and causes the query to time out. This issue has now been fixed.</p>

ArcSight Console

Issue	Description
NGS-5144	<p>Previously the HTML text in a payload viewer used non-HTML line breaks. These are now replaced with HTML line breaks: <code>
</code>.</p>
NGS-5114 TTP#65671	<p>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.</p> <p>Ignore the duplicate rows. This behavior is documented in the Console User's Guide.</p>
NGS-4056	<p>The payload value in ArcSight Web was HTML encoded and an XSS vulnerability was encountered. This issue is now fixed.</p>
NGS-3930	<p>Adding a stacked bar chart to a dashboard where this chart was based on a Query Viewer on an Active List would cause the Console to hang. This issue has now been fixed.</p>
NGS-3129	<p>When you selected the geographic view from events in an active channel, both Longitude and Latitude information were shown as 0.</p> <p>This bug is fixed and now the geographic view can show correct information.</p>
NGS-2167 TTP#66337	<p>The server.log file showed an exception when a custom view dashboard was launched on a system running in FIPS mode. This has now been fixed; Custom View dashboards on a FIPS mode system are launched in an external browser.</p>
NGS-1795	<p>On non-Windows platforms, when you viewed dashboards with Custom layout option in the Console, you got an error, "Failed to create embedded browser, launching external browser". This issue has now been fixed.</p>
NGS-1747	<p>On Linux systems, when viewing dashboards, if you selected the Investigate option you would see duplicate menus. This issue has now been fixed.</p>

ArcSight Manager

Issue	Description
NGS-4335	A memory leak in the CORR-Engine caused the Manager to become unresponsive. This is now fixed.
NGS-4202	The Channel would attempt to refresh event information when an initial query for event data timed out, rather than leaving row as "loading event." This issue is now fixed.
NGS-1847	InActiveList condition on a multimapped active list did not work when all fields (both key and non-key fields) were not mapped. This did not affect non-multimapped active lists. The workaround was to map all the key and value fields. This was a partial workaround, because all the mapped fields need to match the values stored in the MultiMapAL. This has now been fixed.

ArcSight Web

Issue	Description
NGS-5145	A report would fail to run if a web user logged in to the ArcSight Web Console and selected a user's email address for 'Email to' option. The problem occurred when the web user was configured with an Active Directory external id. This issue is now fixed.
NGS-4124	Previously, the payload value in ArcSight Web would be HTML encoded. This issue has now been fixed. Without the fix, the payload value with HTML was rendered and an XSS vulnerability was encountered.

CORR-Engine

Issue	Description
NGS-4229	Archive stopped working after Daylight Saving Time ended in Brazil at midnight on 10/22 when the clock was turned back one hour. The following error appeared in the Logger log file: "An archive with duplicate date already exists in the database". This issue is now fixed.
NGS-4082	If the buffer pool was too small, it caused slow channel performance or prevented logging in to the Console with an error message: [ERROR][default.com.arcsight.common.persist.mysql.MySqlNotificationBroker][p urgeOldNotifications] java.sql.SQLException: The total number of locks exceeds the lock table size You could solve the problem by editing the file /opt/arcsight/logger/data/mysql/my.cnf to set innodb_buffer_pool_size = 512M (the default was 128). Then restart all services. This issue has now been fixed.
NGS-1696	Long running queries would be terminated by CORR-Engine due to excessive system resource utilization. Sometimes, this would impact event insertion rate or EPS. This issue has now been fixed.

Installation and Upgrade

Issue	Description
NGS-2654	The ESM Installation Guide lists the incorrect versions of the supported MAC OS for the ArcSight Console. The correct versions should be 10.6 and 10.7, as indicated in the PLD that supports this release.

Management Console

Issue	Description
NGS-2258	The issue with a dashboard rendering slowly in the browser has been fixed in this release.
NGS-2256	This release supports using stacked bar chart in a dashboard.
NGS-2245	<p>In the Custom Layout of a dashboard, if you tried to change the display format of a data monitor, say from "Bar Chart" to "Table" and you saved the dashboard, the next time that you reloaded the dashboard, the data monitor would still display in the "Bar Chart" format. The display format could not be changed in the Custom Layout.</p> <p>This bug has been fixed.</p>
NGS-2184	The issue with a dashboard occasionally not loading predefined background color/image has been fixed in this release.
NGS-1523	User group creation was failing when the user group name field contained '&'. The system now detects '&' as an invalid character and does not create the resource until valid characters are used. This has now been fixed.
NGS-1435	The Pie Chart view of a Data Monitor or Query Viewer used to have a legend area that, if too long, would shrink the pie chart considerably. The pie chart no longer has a legend area.
NGS-1425	The Custom Layout view of a Dashboard, Data Monitor, or Query Viewer displayed in chart view such as bar chart, pie chart or line chart was failing due to an issue with the Adobe Flash Player. The Adobe Flash Player is no longer used.
NGS-1149	When using the Internet Explorer browser to access the Management Console, in the "Dashboards" section of the Management Console, the Close Dashboard menu command appeared enabled even though it was not an applicable command. This issue has now been fixed.
NGS-1072	Displaying EventGraph data monitors from within the ArcSight Console custom layout internal browser is no longer supported. You must launch an external browser from ArcSight Console custom layout or use the Management Console dashboard module in order to view any dashboard with EventGraph data monitors.

Open Issues in this Release

This release contains the following open issues. Use the workarounds noted, where available.

Analytics

Issue	Description
ESM-48858	System audit events, such as those resulting from a rule being disabled by the system, are given a low TTL (time-to-live) value to prevent excessive rule triggering. A single rule can correlate such audit events, but any subsequent chaining rules will be suppressed.
ESM-48307	The DeviceEventclassId for Windows 2008 has the same value as Windows 2003.
ESM-47918	The Threat Response Manager (TRM) occasionally does not return an appropriate response when an update to Quarantine Node by IP command is sent.
ESM-40449 TTP#66622	When exporting events from the Case Details channel, archived events do not get exported.
ESM-39405 TTP#64400	If you create a report whose name contains Chinese characters, then send the report as a PDF attachment, the received email does not display the attachment's name correctly. (The content of the report is correct; only the email attachment field is affected.)
ESM-37810 TTP#61524	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.
ESM-35070 TTP#54507	<p>Verify Rules with Events (replay with rules) does not work for the following types of active lists if one of the test rules adds to the active list and the second test rule uses that data in a condition:</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 and when only one rule is tested. 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-34531 TTP#53435	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.
ESM-29633 TTP#40230	<p>Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (For example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.</p>
ESM-29348 TTP#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 (for example, one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (for example, 24 hours if run once a day).

Issue	Description
NGS-5165	<p>During the conversion of /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Track Closed Case to a lightweight rule, the order of the actions gets swapped. This results in the entries for cases in /All Session Lists/ArcSight Express/Operations/Case Tracking and Escalation/Case Tracking, but not terminated. The Recently Closed Cases viewer in /All Dashboards/ArcSight Express/Operations/Case Tracking and Escalation/Case Status and several of the case tracking reports, particularly /All Reports/ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Overview, will not display the correct data.</p> <p>Workaround: Fix the ordering of the actions in /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Track Closed Case. To do this:</p> <ol style="list-style-type: none"> 1) Edit /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Track Closed Case. 2) Select the Actions tab and examine the On Every Event [Active] trigger. 3) Select and right-click on the Terminate Session List action and select Copy. 4) Click the Remove button on the Rule Editor's menu bar. 5) Right-click the On Every Event [Active] trigger and select Paste. 6) Click the OK button at the bottom of the Rule Editor.
NGS-5136	If the gzip operation should ever fail (particularly if you run out of disk space) that day's archives state will be in error and you will not be able to move it offline.
NGS-4615	The Windows Critical Services Started or Stopped report has an issue with the rendering of the grouped table column. It does not have the table header background.
NGS-4187	<p>Trend tables that exceed 1 GB may cause a signal 11 error in the CORR-Engine.</p> <p>Workaround: Keep trend tables small (< 1G). Trends running on ESM with Oracle were often created to provide improved report performance on a subset of columns. This is no longer needed with CORR-Engine.</p> <p>The best way to reduce an overgrown trend table is to edit the trend and reduce the "retention" period. For the change to take effect, rerun the trend. If the trend data is no longer needed, you can delete the trend and the space that was used by the trend gets freed up.</p>
NGS-3686 TTP#61694	When you try to delete a Trend being used in a Query and in turn used in a Query Viewer, you will get an error and the Trend will not be deleted. This is a dependency chain. Remove the use of this trend in other resources first before using it.
NGS-3294	Base events cannot be retrieved from the source Manager by the destination Manager.
NGS-3139	<p>While trying to query on a Case, specify the ID of the user instead of the name of the user.</p> <p>For instance,</p> <p>owner=admin --- won't work</p> <p>owner=1UOtZMTkBABCA0qd7zsU1IQ== --- will work</p>
NGS-2917	<p>When a lightweight rule is scheduled, the rule actions that update data lists may not work correctly if the fields mapped to the list columns are not used in any rule conditions.</p> <p>Workaround: Add a simple condition on the mapped fields. For example, if field DeviceCustomNumber1 is used in the mapping for an AddToList action, add a rule condition such as "DeviceCustomNumber1 IS NOT NULL". Then, the field value for that event will be queried from the database when the scheduled rule task is executed.</p>

ArcSight Console

Issue	Description
ESM-49990	To display the correct icon for forwarded correlation events, add the Locality Field column to the field set of the channel.
ESM-49187	The Text (Column Names/Field Names/Aliases) in the Table Header do not display CJK characters even if the table has been set to use Arial Unicode MS font.
ESM-47213	<p>Case-related events are copied to a special table so they can remain available after being archived. The channel is unable to find and display such events correctly after the partition is archived.</p> <p>Workaround: Use the case event editor or Reports, which can correctly find and display these events.</p>
ESM-41641 TTP#69565	<p>On Macintosh only: If you open a channel, select some rows, right-click on them and select Print Selected Rows from the resulting menu, it causes the Console to crash.</p> <p>Workaround: Before you start the Console, make sure to set up a default printer to which to print. This problem occurs when you do not have a printer set up.</p>
ESM-41019 TTP#67856	<p>When you have client-side authentication set up, if the Manager is configured with the "Password Based and SSL Client Based Authentication", you will get an error when accessing the product documentation using both the embedded browser in the Console as well as the external browser.</p> <p>Workaround: Generate a key pair for the browsers and import the browser's certificate into the Manager's truststore. Alternatively, copy the Console's key into the browser's keystore. See the Administrator's Guide for details on how to do this.</p>
ESM-40587 TTP#66906	<p>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.</p> <p>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.</p>
ESM-39980 TTP#65708	The Console can become unresponsive if you access other resources while building category models with a large number of actors.
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: Resize the panel before running a report. You may want to try several resizings to get the desired results.</p>
ESM-39829 TTP#65421	Deleting actors will require category models, if any, to be re-built. Each rebuild may take seconds. So, when thousands of actors are deleted, the whole deletion period may last for hours since actor deletion launches a category model rebuild.
ESM-39331 TTP#64251	Actor channels can only display fields that are part of a pre-defined field set. If you want to view any additional fields in an Actor channel, first add the fields to the field set that the Actor channel uses instead of adding them directly to the channel.
ESM-38961 TTP#63568	<p>In the Image View mode, when a background file is uploaded, the Console does not provide an option for a location. The file automatically gets uploaded into your personal folder.</p> <p>Workaround: After the upload, move the file to a preferred folder.</p>

Issue	Description
ESM-37344 TTP#60500	<p>On the Manager, when a large number of cases reside in a single group, you can't pick a case for "Add to Existing Case" rule action in the Rule editor. This is because the resource selector only shows leaf nodes when there are less than 1000 cases in a group. This happens for all resources.</p> <p>Workaround: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.</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>
ESM-33440 TTP#51072	<p>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.</p>
ESM-33360 TTP#50968	<p>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.</p>
ESM-32705 TTP#49608	<p>In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range.</p> <p>Workaround: Delete the existing color mapping and create a new one with the color mapping of your choice.</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> <p style="padding-left: 40px;">^VVsOXg4BABCAIEuBhILMyg==</p> <p>Enter</p> <p style="padding-left: 40px;">"^VVsOXg4BABCAIEuBhILMyg=="</p> <p>in the query text field.</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>
NGS-4811	<p>Certain resources in ArcSight Express are linked from other content groups, such as ArcSight Foundation or ArcSight Administration. For such resources, the ArcSight Console and the ArcSight Express Standard Content Guide show the parent URIs; for example, All Dashboards/ArcSight Foundation/NetFlow Monitoring/NetFlow Bandwidth Usage Overview instead of All Dashboards/ArcSight Express/NetFlow Monitoring/NetFlow Bandwidth Usage Overview.</p> <p>You can see the parent URI for a resource on the ArcSight Console either from the Inspect/Edit panel when you edit a resource or by resting your mouse on the resource in a use case. If the parent URI points to content for which you do not have permissions (for example, the ArcSight Foundation content is available to ArcSight Administrators but not to ArcSight Express users), the Find Resource in Navigator command does not display the resource in the Navigator.</p> <p>Workaround: Use the Use Case resource to run reports, see dashboards, and so on.</p>

Issue	Description
NGS-4611	On ArcSight Console only: When uploading a background in Custom Layout Mode, "Browse..." button might not work. If this happens, upload the background using the Management Console instead.
NGS-4091	If the arc_notification_history and arc_notification_registry are too big, the ArcSight Console will hang.
NGS-4078	When using the ArcSight Console on Windows 7 and 64-bit machines: Opening a dashboard in Custom Layout might result in the dashboard not loading promptly. Workaround: You can either re-size the window or undock the Viewer to make the dashboard render again.
NGS-4060	On ArcSight Console only: When viewing a dashboard such as "/All Dashboards/ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Executive View" in Custom Layout mode, the titles may appear to be cut off. This happens because the window is too small to show its entire contents. Increasing the size of the window should solve this issue. If the issue still persists, open the dashboard in an external browser.
NGS-3850	If you have trouble with the internal browser on a Win64 system, please use the external browser.
NGS-2499	The time field in the Image Dashboard will be displayed as a number instead of displaying as formatted date and time. Workaround: Use regular dashboard instead of Image Dashboard.
NGS-2241	When you first create or view a new custom view dashboard with one or more data monitors or query viewers, the dashboard elements might overlap. Workaround: Define the arrangement and save it. This can be done in one of these ways: 1) Using auto-arrange: Go to Edit->Auto Arrange and then click 'Save' to preserve the changes. 2) Manual arranging: Go to Edit->Arrange and move/resize all dashboard elements to the desired position. When finished, click 'Done Arranging' and then 'Save'.
NGS-1745	This affects Arcsight Console Dashboard in custom layout mode, and Management Console dashboards. When viewing a dashboard such as "/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status", if the DataMonitors and/or Query Viewers seem to be overlapping each other, click on Edit->Auto-Arrange. This will arrange the dashboard again such that all dashboard elements are correctly displayed. Save the dashboard.
NGS-1262	If a dashboard contains a Query Viewer that has a large row limit, the Console may hang while loading this dashboard in Custom Layout view. It is a good practice to keep the row limit of Query Viewers to less than 100 before viewing the dashboard in custom layout format.
NGS-1088	If a regular or inline filter with a condition involving Event Annotation Flag is applied to an Active Channel, the Active Channel will not load any events. Workaround: Avoid using Event Annotation Flag in filter conditions.
NGS-146	Occasionally, event-based Active Channels that include InCase filtering condition will not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit. This issue will rarely be seen because the CORR-Engine provides powerful event compression and it can support very long retention periods given sufficient disk space. This reduces the chance of events expiring while bound to an open case.

ArcSight Manager

Issue	Description
ESM-47625	During case export, the Creation Time was changed to the time of the export. The creation time is no longer reset.
ESM-41331 TTP#68451	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: To produce a correct report, run the resource validation script manually as follows:</p> <ol style="list-style-type: none"> 1. Run the script using 'arcsight resvalidate' 2. Run the script again using 'arcsight resvalidate -persist false' <p>In general, if you need to run the resource validation script, you have to run it twice: the first time with '-persist true' (default) to validate and fix invalid resources, and the second time with '-persist false' to generate a correct report:</p> <pre>arcsight resvalidate arcsight resvalidate -persist false</pre>
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-37488 TTP#60808	<p>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 file. Additionally, the Manager runs out of memory and therefore automatically restarts itself.</p> <p>Workaround: 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.</p>
ESM-33462 TTP#51112	Stages resources are editable from the ArcSight Console, although these should not be moved or customized. (See the ArcSight Console Navigator > Stages resource tree) 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.
ESM-31433 TTP#46276	<p>You may see the following exception in the Manager's log file:</p> <pre>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</pre> <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 Manager's 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's log file:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Re-generate the index by issuing the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create</pre>

Issue	Description
NGS-4837	With certain long running queries it is possible for a deadlock to occur in the JDBC driver. You may notice this by a decreased throughput. If you suspect this, you should request a thread dump through the Management Console and see if the dump indicates a deadlock (at the end of the dump, it would specifically say "deadlock"). If a deadlock does occur and is an issue for you, you will need to restart the Manager to resume normal operations.
NGS-3856	When displaying an Active List with a large number of entries (for example, 10 million entries), you see an error in the server.log file. Workaround: Increase the memory size for the Manager to ensure that the Active List size is within limit. Also, if possible, avoid displaying Active Lists with a large number of records.
NGS-3825	If the field size of an event exceeds 32 KB, that event does not get persisted.
NGS-3803	The command, "arcsight manager-reload-config" fails to dynamically reload the configuration. Restart the Manager if you make any configuration changes such as the ones that go in the config/server.properties file.
NGS-3771 TTP#52583	A new feature in this release automatically deactivates any user account that has been inactive for more than 90 days. After installing the product, run the "arcsight managersetup" command to implement this feature. Then restart the Manager. To change the inactive period, add the property auth.user.account.age= <days> to the Manager's server.properties file, change <days> to the number of days you want, and restart the Manager.
NGS-1937 TTP#56123	The Archive tool can occasionally fail to import entries into an active list due to transient errors. In such situations, you may not see any errors, but the list does not get populated. Workaround: Re-import the same package.
NGS-1449	When you shut down the services using the arcsight_services command, you may see exceptions in the log file. These exceptions are generated due an issue with the order in which the components are shut down and can be safely ignored.
NGS-264	When integration with iDefense is enabled and you create a Case in ArcSight Express, the Case notes may have some special characters garbled. The text can alternatively be viewed in iDefense or in the Event Inspector panel.
NGS-172	Base events do not get annotated automatically after rules trigger. Workaround: Annotate the events manually.

ArcSight Web

Issue	Description
ESM-41321 TTP#68431	If the report name contains the hash character "#", there may be a problem displaying the report correctly. In such a case, remove the "#" character from the report name.
ESM-35801 TTP#56258	If you create a Case and set the Estimated Resource Time in ArcSight Web, it does not get set. Workaround: Define this setting on the Console. See the Console online Help for steps to do this.
ESM-33922 TTP#52336	On ArcSight Web, there is no row limit imposed on Query Viewer chart displays (unlike on the ESM Console). Query Viewer charts with more than 100 rows do not display properly and are virtually unreadable. On the ArcSight 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 rows beyond the 100th row will not display properly on the Web. Workaround: In the Console, set row limits on Query Viewers. This will control chart displays in the Console and ArcSight Web. Determine which Query Viewers you want to display as charts. In the ArcSight Console, edit those Query Viewers to set the Row Limit to 100 (or less). To do this: 1. Log in to the ArcSight Console. 2. Select Query Viewers in the Navigator. 3. Right-click the Query Viewer you want to edit. 4. In the Query Viewer Editor, if Use Default is enabled, click to deselect it. 5. Enter a row limit of 100 or less. 6. Click Apply or OK to save the changes.
NGS-4462	We recommend running sendlogs from the ArcSight Console, or from the Manager directory (/opt/arc sight/manager). Running sendlogs from ArcSight Web directory (/opt/arc sight/web) is not recommended, it fails to collect remote logs (Manager, database, and connector logs).
NGS-3990	Occasionally, when you select the Knowledge Base link in ArcSight Web, navigating the user interface fails to work correctly. Workaround: Log out of ArcSight Web, clear the browser cache, then log back in.
NGS-3989	The ArcSight Web Login banner displays newline characters as \n instead of adding a new line.
NGS-3605	The Management Console does not support a user-configurable banner which is commonly used to display custom login messages.

CORR-Engine

Issue	Description
NGS-4790	<p>In case your database fills up, there are a number of ways to free up space:</p> <ol style="list-style-type: none"> 1. You can delete any unused trends. Deleting the trend will free up any data in the table associated with this trend. 2. You can reduce the retention period of specific trends. By default, trends keep 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time this trend runs. 3. You can examine the contents of your session lists. Data is not usually removed from session lists. Running "bin/arcsight dropSLPartitions -h" will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.
NGS-1429	You can only restore archives from a single CORR-Engine. Do not combine archives residing in multiple CORR-Engines.

Connector Management

Issue	Description
NGS-5124	<p>If you used a proxy server to get to the Protect 724 ArcSight Community, ArcExchange displays the following authentication error when configuring the host information for arc-exchange in order to remotely manage the appliance:</p> <p>"The code can't reach Protect724.arcsight.com"</p>
NGS-4643	<p>Abrupt Operating System shutdown (as caused by power outages or cold/hard reboot) may corrupt the Connector Management configuration. This may cause previously added locations, hosts, and containers to disappear altogether. To prevent data loss, we recommend that the customers periodically back up their connector configuration. This can be done by clicking on the 'System' node in the navigation tree, and selecting the 'Export Remote Management Configuration' (icon 'Down Arrow'). This will save the configuration in an '.aup' file which can be used to recover any lost data.</p> <p>To restore back the data, the customers need to perform the following steps:</p> <ol style="list-style-type: none"> 1. Stop the conapp service 2. Delete the connector_config.xml in /opt/arcsight/conapp/userdata/conapp directory 3. Start the conapp service 4. Upload the Remote Management Configuration the customers saved <p>This can be done by clicking on the 'System' node in the navigation tree, and selecting the 'Import Remote Management Configuration' (icon 'Up Arrow').</p>

Connectors

Issue	Description
NGS-5137	Setting of eventpollcount did not retain for each host after deleting some Windows host(s) from agent setup wizard.
NGS-5111	If a syslog SmartConnector runs out of disk space, it may not be able to process any more events until it is restarted. Events arriving during this period will be permanently lost.

Issue	Description
NGS-3806	<p>Auto-import of the Manager's certificate does not work if your connector is installed in FIPS with Suite B mode.</p> <p>Workaround: Import the Manager's certificate manually. Refer to the Configuration Guide for instructions on manually importing the Manager's certificate into the connector.</p>
NGS-3498	<p>The certificate auto-import feature in connectors will only import certificates from the initial configuration.</p> <p>Workaround: Any changes or additions to the destinations require you to manually import the certificate for those destinations.</p>
NGS-2052	<p>When using Asset Model Import Connector to import assets, the connector does not uniquely identify assets by Zone and a unique IP address or a unique host name.</p> <p>For updating existing assets, please make use of one of the following attributes to identify them:</p> <ul style="list-style-type: none">- An External ID, or- a resource ID, or- a URI
NGS-1423	<p>On Windows machines, while a connector is being upgraded from the ArcSight Console, if any process is using the connector's 'current' folder, the upgrade fails.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Make sure that you don't have any files in the connector's 'current' folder open.2. Do not start the connectors using the 'arcsight agents' command. Instead, start the connector from <Start> -> <Programs> -> <Connector Programs>

General

Issue	Description
NGS-4712	<p>The following exception in the server.log of the Manager:</p> <pre>com.arcsight.common.persist.PersistenceException: Unable to execute query: Incorrect key file for table '/opt/arcsight/logger/data/mysql/#NNNNNNN.MYI'; try to repair it where NNNNNNN are arbitrary characters denoting a temporary table name</pre> <p>This is an indication that MySQL ran out of disk space during the execution of a query. The query in question can be a query executed by a direct user request, such as a Query Viewer or a report. The query can also be a query executed as a part of a system task, such as a Trend. The query could run out of disk space because it requests processing a large event time range. Reducing the time range of the query will help. It will also allow the query to execute faster.</p> <p>Also, the query could run out of disk space because it competed for the disk space with the other queries running at the same time. Try to re-schedule the Report tasks in such a way as to avoid multiple reports running at the same time.</p> <p>For troubleshooting Trend queries, refer to Query and Trend Performance Tuning section of the Administrator's Guide.</p>

Installation and Upgrade

Issue	Description
NGS-5128	For upgraded systems, an empty group, Trends Status, may appear under /All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Trends. This empty group can be safely deleted or ignored.
NGS-5050	<p>The following rules may be in a disabled state after upgrade from AE 3.0 to AE 4.0. You can enable them as needed after upgrade.</p> <ul style="list-style-type: none"> /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Case Deleted /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Case Escalation /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Case Investigation Started /All Rules/ArcSight Express/Operations/Case Management/Case Tracking and Escalation/Monitor New Case /All Rules/ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Deleted /All Rules/ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Escalation /All Rules/ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Investigation Started /All Rules/ArcSight Foundation/Workflow/Case Tracking and Escalation/Monitor New Case /All Rules/Real-time Rules/Workflow/Case Tracking and Escalation/Case Deleted /All Rules/Real-time Rules/Workflow/Case Tracking and Escalation/Case Escalation /All Rules/Real-time Rules/Workflow/Case Tracking and Escalation/Case Investigation Started /All Rules/Real-time Rules/Workflow/Case Tracking and Escalation/Monitor New Case

Issue	Description
NGS-4874	During the resource upgrade or migration from 5.0 SP2 Patch 4 to AE 4.0 some exceptions related to the references to deprecated resources show up in the logs even though the resources are all valid.
NGS-4782	After upgrading to ArcSight Express 4.0, the custom ArcSight Express users still have access to some ArcSight Foundation resources that were available in ArcSight Express 3.0 (for example, /All Queries). Due to upgrade process issues for ACLs in user groups, we recommend that you remove the access permissions to /All Queries for the users in /All Users/Custom User Groups/ArcSight Express. Permissions to /All Queries is not necessary, and has been replaced with permissions to /All Queries/ArcSight Express.
NGS-4582	<p>The following data monitors may be in a disabled state after upgrade from AE 3.0 to 4.0 depending on whether they were enabled or disabled in AE 3.0. You can enable them after upgrade and use them.</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Configuration Modifications/Host Configuration Change Event Counts by Zone</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Configuration Modifications/Last 20 Host Configuration Modification Events</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Configuration Modifications/Most Common Host Configuration Change Events</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Problems Overview/Host Problem Event Counts by Zone</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Problems Overview/Last 20 Host Problems</p> <p>/All Data Monitors/ArcSight Express/Operations/Configuration Changes/Host Problems Overview/Most Common Host Problem Events</p>
NGS-3445	In some situations, the Installer panel may indicate that the installation is successful while the Web Server fails to start. Refer to the Administrator's Guide on how to manually configure and start the Web Server.
NGS-3322	<p>Due to the timing of some components' start-up, there may be some harmless error messages in the log files such as:</p> <p>[FATAL][default.com.arcsight.logger.distributed.DirectConnection\$ReadChannel][run]</p> <p>java.io.IOException: end of communication channel</p> <p>[FATAL][default.com.arcsight.logger.distributed.ClientDirectConnection][run]</p> <p>java.nio.channels.ClosedChannelException</p>
NGS-3067	When configuring the product using the First Boot Wizard, if you use a wrong IP address or an unresolved IP address in the Manager Hostname panel, the First Boot Wizard will continue installing but fail during Arcsight Web configuration. Make sure the Manager's hostname or IP address is correct and can be resolved otherwise the Manager will not start.

Localization

Issue	Description
NGS-4220	<p>In the Traditional Chinese localized environment, the Reports display some messy code.</p> <p>To work around this issue:</p> <ol style="list-style-type: none"> 1. Log in to ArcSight Console and open the report. 2. Create the report with a Chinese name. 3. Select the report template. 4. Edit the template with "Open in designer." 5. Edit the header and other fields which need to display in Chinese characters. 6. Set the fonts to Arial Unicode for the fields that need to display Chinese characters. 7. Save the template. 8. Run the report with PDF format. 9. Open the generated report with Acrobat Reader version 9 to check if the Chinese characters display properly.
NGS-2435	<p>For non-English locale environments, only English characters are supported for user name and password. Using non-English characters for user name and password might result in authentication issues.</p>

Management Console

Issue	Description
NGS-5134	<p>On the Management Console of ArcSight Express 4.0, you cannot enter a password which is greater than 16 characters long in the password field.</p> <p>The implication of this is that if a you change your password via the ArcSight Web Console to something with more than 16 characters, you will not be able to log in to the Management Console.</p>
NGS-3892	<p>In the Management Console, Dashboards that contain a Data Monitor of type 'System Monitor' or 'System Monitor Attribute' will display only the first 100 rows.</p>
NGS-3858	<p>The minimum and default heap size for the Manager is 8 GB, the maximum heap size is 16 GB. You can change this size based on total available memory on your system. The error message related to this heap size in the Management Console does not reflect this accurately. If you need to configure the heap size beyond 16 GB, please contact HP ArcSight Customer Support before doing so.</p>
NGS-3084	<p>Global variable fields do not get displayed in an Image Dashboard.</p>
NGS-2849	<p>If the refresh rate is set to a low interval so that the refresh happens too frequently, under slow network connections or when having network problems, this might impact browser performance and dashboard behavior. To avoid this problem, set the refresh rate to a higher value. You can manually refresh the dashboard if needed.</p>
NGS-2301	<p>The Management Console does not support 3D bar charts.</p>

Issue	Description
NGS-1582	In the Management Console's Advanced Permissions dialog, if you choose to set permissions on the Field resource, you may see a hidden folder called customCells under your personal folder. This will only appear if you have created some customCells using the ArcSight Console. If you see such a folder, do not change the ACL settings on it. Doing so will affect the working of custom cells in ArcSight Console.
NGS-1451	If a custom view dashboard contains a query viewer with a large row limit, the browser may hang while loading this dashboard. It is a good practice to keep the row limit of Query Viewers below 100 before viewing the dashboard in custom layout format.
NGS-1283	You must have administrator privileges to access the user/connector management feature.
NGS-1275	The Notification Groups attribute is missing from the Connector Management page. Workaround: Use the ArcSight Console to view the Notification Groups through the Configure Connector option.
NGS-1256	In the Management Console, after clicking the tab to navigate into a module, you may encounter a blank screen. Workaround: Refresh the screen by reloading the browser page.
NGS-1254	When using some versions of the Firefox browser, occasionally your login fails and you see the following exception in the server.log file: " java.lang.SecurityException: Blocked request without GWT permutation header (XSRF attack?)" This happens because of an issue in Firefox which occasionally drops GWT headers beginning with x. Workaround: Add the following property to the server.properties file: cross.domain.enabled=true and restart the Manager in order for it to take effect.
NGS-277	You cannot select the docked items (icons such as admin, dashboards etc.) using the keyboard shortcuts. The only way to select them is by using the mouse.

Pattern Discovery

Issue	Description
ESM-35048 TTP#54452	A java.lang.InterruptedOperationException might be logged in the Manager's server.std.out.logs file 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.
NGS-3527	Pattern Discovery jobs can be resource intensive. Under high EPS, Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. ArcSight recommends that you reduce the number of events over which the Pattern Discovery search runs and/or frequency of Pattern Discovery jobs when running a system with high EPS.