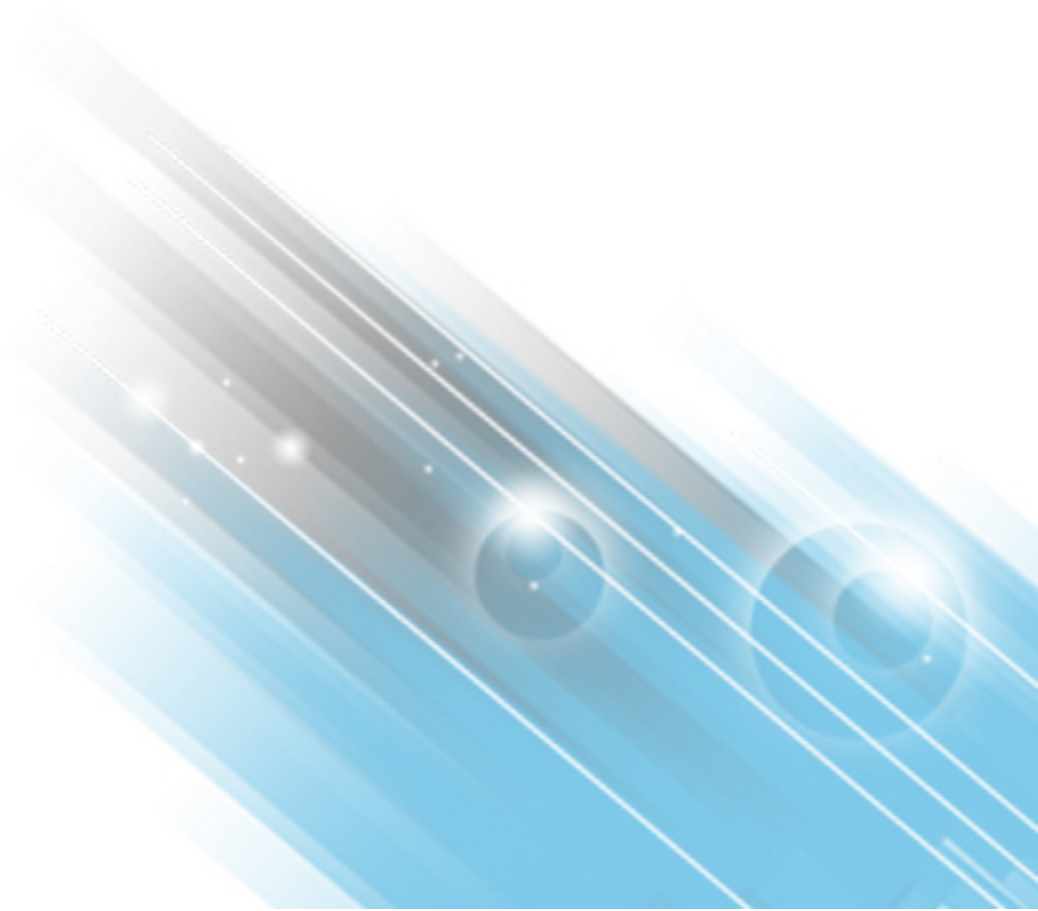
HP ArcSight ESM Express

Software Version: 6.9.0c

Release Notes



August 18, 2015

Legal Notices

Warranty

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.

The information contained herein is subject to change without notice.

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

ArcSight ESM Express 6.9.0c

Welcome to ESM 6.9.0c

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

ESM includes the Correlation Optimized Retention and Retrieval (CORR) Engine, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

What's New in This Release

This topic describes the new features and enhancements added in ESM Express 6.9.0c.

ArcSight Command Center

New Tool Command Utilities to evaluate the Network Route of an Event

ArcSight Command Center now provides utilities, called Tool Command utilities that enable you to evaluate the connections on the network used by a Channel event.

Active Channel Improvements

The following improvements have been made to Active Channels. You can:

- Add to, and remove, field columns from the Channel Grid.
- Create, edit, and delete Event Channels.
- Apply Filter Conditions to Event Channels.

BETA: New metrics available, Average EPS and Average GB

ArcSight Command Center now displays two metrics in the navigation header: Average EPS and Average GB. These metrics provide the average events per second processed and average size of event data received per day, respectively. These metrics are collected and reported for the most recent 30 days of data.

Refer to the ArcSight Command Center User's Guide for more information.

ArcSight Console Enhancements

Enhanced Active List option on active channel

You can now add your favorite active lists to the right-click Active List menu on the active channel, saving you the extra steps of drilling down through the resource tree selector to select your list from various list groups. Create your favorite active list collection using the Console's Preferences menu.

Refer to the topic, "Customizing the Selections for Active Lists" in the ArcSight Console User's Guide.

Correlation Enhancement: Rule Resilience

In this release, a resource-intensive deployed rule that causes EPS rates to drop is automatically disabled. The threshold for disabling is 50% of aggregate evaluation time of deployed rules.

For information on how to change the threshold setting, refer to the topic, "Automatically Disabled Rules," in the Reference Guide section of the ArcSight Console User's Guide.

New Type Conversion Functions

The following Type Conversion functions are introduced in this release:

- ConvertStringToResourceReference
- ConvertStringToIPv6Address
- ConvertStringToMACAddress
- ConvertStringToDate

Use these functions to convert data types in your rules. Refer to the descriptions for Type Conversion functions in the topic, "Variable Functions," in the ArcSight Console User's Guide.

List Enhancements

Active Lists

You can now include the *Count*, *Creation Time*, and *Last Modified Time* fields in your active lists in rule conditions.

Session Lists

A new session list attribute, *TTL Days*, enables you to set the number of days a closed session should remain on the list, after which the session is removed.

Refer to the topic, "List Authoring," in the ArcSight Console User's Guide.

zoneUpdate Administrative Command

You can now use the optional `zoneUpdate` command to update IPv4 address allocations and dark space information that are provided in the periodic Zone Update Subscription Package. You can use `zoneUpdate` after a successful Manager installation or upgrade. This command is available from the command line only, and has no GUI functionality.

`zoneUpdate` performs these actions in the Global network:

- Makes an inventory of affected assets
- Removes old zones
- Installs and updates zones
- Auto-zones assets

The `zoneUpdate` command updates zones in the Global network only. Local zones are not updated by this command. The behavior of `zoneUpdate` is the same for both dynamic and static zones.

Refer to the topic, "zoneUpdate", in the Administrative Commands appendix of the ESM Administrator's Guide.

HP ArcSight now offers Security Use Case packages available for download at https://arcsight.hpwsportal.com/catalog.html#/Home/Show. These packages provide essential security monitoring for network systems (such as IDS/IPS, VPN, Firewall), and packages that monitor and analyze the event stream for critical security concerns, such as anomalous traffic and suspicious outbound traffic. HP ArcSight IPv4 Internet Dark Zones Update Version 2.0.0.0 is also available for download.

Beta Feature: Superindexes

Superindexes is a feature available to qualified customers on a test basis in ESM 6.9.0c. This is a Beta feature which is limited to specific environments and configurations. It is disabled by default.

Superindexes enable ESM to determine quickly whether a particular field value has been stored in the database, and if it has, to narrow down the search to sections of data where that field value exists.

Searches that can take advantage of superindexes return results quickly if there are no hits. Superindexes also return results more quickly than regular searches when there are few hits (rare values), and are therefore excellent for needle-in-a-haystack searches. Searches on fields that are not superindexed will be returned at normal speeds.

Consult with your HP Solution Architect to contact Product Management to determine eligibility to participate in the Beta and activate this feature.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20150601.

Vulnerability Updates

This release includes recent vulnerability mappings from the June 2015 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU-1304 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Cisco Secure IDS S872 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB, MSKB
Juniper / Netscreen IDP update 2500 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB, MSKB
McAfee Intrushield updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, CERT, MSSB
TippingPoint UnityOne DV8719 updated	Faultline, Bugtraq, CVE, Nessus
IBM Enterprise Scanner 1.133 updated	CVE, X-Force
IBM Security Host Protection for Desktops 3140 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 35.060 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3140 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 35.060 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 35.060 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Server IPS for Linux technology 35.060 updated	Faultline, CVE, Nessus, X-Force
IBS RealSecure Server Sensor XPU 35.060 updated	Faultline, CVE, Nessus, X-Force

Device	Vulnerability Updates
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	Bugtraq

Supported Platforms

See the ESM Support Matrix document available on the Protect 724 site for details on ESM Express 6.9.0c platform and browser support.

Supported Languages

These languages are supported by ESM:

- English
- French
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean
- Russian

Usage Notes

Asset Model Import FlexConnector

The Asset Model Import FlexConnector supports the ability to create and manage the Asset Model within ESM. The Asset Model Import FlexConnector allows you to develop a model import connector to import asset model data from a file. This enables you to create and maintain ESM Network Model data and keep the data in sync with the data in your Asset Management system. The Asset Model Import FlexConnector to install for ESM 6.9.0c is version 7.1.2.7395.0. See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.9.0c supported platforms.

Forwarding Connector

The Forwarding Connector can receive events from a source Manager and then send them to a secondary destination Manager or to an ArcSight Logger. The Forwarding Connector to install for ESM 6.9.0c is version 7.1.3.7495.0. Only the Linux executable applies to ESM 6.9.0c. See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.9.0c supported platforms.

Domains

The Domains feature is not supported for this release.

Running Concurrent Searches

The number of concurrent searches is limited by the capacity of the event reader. By default, the maximum capacity for the event reader is 4. So the system will perform well with 4-6 concurrent searches. If you want to run more concurrent searches, increase the event reader capacity and the Java heap size for the Logger server.

Scroll Bar Issues with Google Chrome and Apple Safari

When using the Chrome or Safari browser, scroll bars may appear inside the data grid on the Storage Mapping tab when the page is loaded for the first time. Adding another row eliminates the scroll bars. Subsequently, adding or deleting rows works as expected.

Trend Tables

Trend tables do not support the display of list elements. For example, if you create a query that uses a Group variable (such as GetGroupsOfAssets and FormatGroupsOfAsset) to return list values, and you create a trend using that query, your trend displays a single element instead of a list of elements.

Localization

In some locales, some text strings may not be translated and display in English. These untranslated strings do not affect functionality and will be addressed in the next release.

Open Channels in the ArcSight Command Center

Event channels, which are the type that Command Center supports, can be resource intensive at times. Those with a time range of an hour or so are an example of this. If a channel takes long to load in a high-traffic environment, open this channel in the ArcSight Console. To view a resource-intensive channel in Command Center, narrow the time range to 5 – 10 minutes to reduce the event volume.

For optimum performance in high traffic environment, limit open channels to 3 per browser, though the limit for channels per browser is 10. Command Center can support up to 15 less intensive channels and between the ArcSight Console and ArcSight Command Center, limit open channels to 25.

ESM Express Unsupported Features

These features are not supported by ESM Express:

- High Availability
- Risk Insight
- Pattern Discovery
- Actors
- Peer relationship feature (including content synchronization)

Mac OS X Console Does Not Support FIPS Mode

The Mac Console does not support FIPS Mode.

Menu Items Inaccessible in ACC Resized Window

For displaying the ArcSight Command Center, use a monitor that has a width of at least 1450 pixels. This is the minimum width needed to display all of the top-menu items without rendering the menu items inaccessible. This minimum width also applies on a larger monitor when reducing the size of the browser window.

Upgrade Not Supported

Upgrade is not supported for the ESM 6.9.0c release. This version of ESM cannot be upgraded from other ESM Express versions. It can be installed on a new ESM Express server only.

Content Synchronization Not Available; Requires Peer Relationship Feature

In the ArcSight Command Center, Content synchronization is not available for this release because it requires the Peer relationship feature, which is not supported (license enabled) in ESM Express.

Open Issues

Analytics

Issue	Description
ESM-49436	Filters having conditions on Variables that return an Actor list field cannot be used in Queries and Active Channels. You can only use these filters in Rules and Data Monitors. This issue affects content developers using Variables in ESM.
ESM-49283	When defining filters, for a hostname to be properly interpreted from the Request URL, the host name needs to be enclosed either within // (double slash) and / (single slash); or within // (double slash) and : (colon). For example: https://hostname.example.com:8443 Such an event is retrieved correctly with the 'Request Url Host Is Not Null' filter. Do not use a filter with a condition that says 'Request Url Host != Null' because != makes the filter invalid.
ESM-39405	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	For scheduled reports, when the user's "Run as" 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-29633	Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid. 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.
NGS-7181	Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.

Issue	Description
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.

Analyze/Search

Issue	Description
NGS-8530	In the Command Center search feature, some expected fields are missing from exported search results. For example, search for events, click Export Results, and check All Fields in the page Export Options, then click Export and download the exported results. In these results, only some basic fields are listed, such as endTime,Name,sourceAddress, and others. Workaround: In the ACC search page, after a search is completed -> click on export. Instead of selecting the checkbox to include all fields, enter a comma-separated list of fields in the text area provided.

ArcSight Console

Issue	Description
ESM-48207	The context menu for Query Viewers in Image Dashboard is specific to Data monitors and may not work.
ESM-47495	Custom Layout Dashboards now support Query Viewers, however, the toolbar in each dashboard and the left-click context menus still use the "Data Monitor" menu label, although Query Viewers are also available from this link.
ESM-47489	If you add a Query Viewer with a default row limit of 10,000 to a dashboard, the dashboard may not load in Custom Layout. The reason is that the Custom Layout is web based and requires a web browser to work. Most web browsers can't handle such large amount of data. Workaround: Reduce the row limit before adding the Query Viewer to the dashboard.
ESM-41344	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. Workaround: Click No to dismiss the message. You may also refresh the page.

Issue	Description
ESM-41019	When you have client-side authentication set up, and if the Manager is configured with the Password Based and SSL Client Based Authentication, an error will be returned when accessing the product documentation using a Web browser. Workaround: Generate a key pair for the browsers and import the browser's certificate into the Manager's trust store. Alternatively, copy the Console's key into the browser's keystore. See the Administrator's Guide for details on how to do this.
ESM-40587	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-38014	When a filter is moved from one group to another and data monitors that depend on that filter are packaged, exported, and re-imported on a different ESM installation, the data monitors may lose some filter attribute values. Workaround: Manually specify the filter again for data monitors that are identified by the broken resource icon.
ESM-37344	On the ArcSight Console, when a large number of cases reside in a single group, you can't pick a case for the "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. Workaround: Arrange the resource hierarchy so there are no more than 1000 resources in a single group. Alternatively, use a dynamic case name (a case name that includes a variable) in your rule action to specify the case. In the ArcSight Console User's guide, search for "Dynamic case name" in the "Rules Authoring" chapter.
ESM-36055	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, when such query is used in query viewer or report it will not show data.
NGS-14227	In a Non-English installation in the Console, if you create a case and then immediately select Add to Case/Case in Editor, the events may not be added to the newly created case. Workaround: Save and lock the new case before adding events to it.
NGS-14191	When you run the Database Performance Statistics dashboard in an environment that has a local language other than English, you may see two sets of entries in the Database Free Space area: one in the local language used by ESM, and the other in English. If this happens, both the ArcSight Console and the ACC will be affected.

Issue	Description
NGS-14188	ESM Console installation on non-English path in Windows machines fails to configure Console. Workaround: Use English filenames in installation paths. Or run Console configuration after installation finished by running consolesetup script from Console ..\current\bin directory.
NGS-13910	Data monitor:/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/CPU Sensors might have no data, because the audit events from Logger has been changed, and it will be fixed in the next release.
NGS-13896	In the ArcSight Command Center you can display license information. The Connector Appliance is no longer part of ESM Express, so the license no longer uses the related flags. Ignore the following entries in the displayed license information: - Connector Management Enabled - Local Connector Limit - Remotely Managed Connector Limit
NGS-13829	Stages resources are erroneously not locked as system content and are editable from the ArcSight Console, on the resource Navigator > Stages resource tree. Do not customize or move these stages resources, as doing so might cause the Manager to become unusable. The system content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.
NGS-13800	In Advanced Editor for InGroup operator, for an asset, select only an asset or asset category. Selecting a zone will not retrieve any information as an asset does not have a relationship with a zone group. This is for both Console and the ArcSight Command Center.
NGS-11278	When a Non-Admin User attempts to use an Active Channel filter to find cases using the Outcome After Research value in field = 'unauthorized activity', the active channel displays Loading resources in the name field, then changes to loading and hangs. In addition, the correct number of total cases is displayed in the upper right corner; however, the cases are not displayed in the channel.
NGS-11212	On the Case Editor's Notes Tab, if you entered non-English characters such as Russian, German, or Portuguese, ESM added them in an unreadable encoding.
NGS-11153	The console starts up successfully, but with the error message "Cannot find sree properties in /home/arcsight/Console/current/reports/sree.properties." Workaround: Ignore this message.
NGS-8630	Not all drill-downs will be valid. A drill-down definition can be based on all available attributes, but when viewing a query viewer in a chart, not all attributes will be displayed. So a drill-down definition based on an attribute that is NOT part of a chart view will be invalid. In that case, the query viewer must be viewed in a table.

Issue	Description
NGS-7735	An overlapping session list contains duplicate entries for the same key field. The session list is part of variable definition and used in filter. If the filter is used in active channel and the session list entry is deleted, the deleted entry may continue to be displayed on the active channel. This condition is temporary and eventually the channel will be updated.
NGS-7173	The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.
NGS-5981	When annotating groups of events, the count of events which the Console indicates were updated may not reflect the correct number of updated event records.
NGS-3084	Global variable fields of the type "GetActiveList" are not displayed on custom layouts and Image Dashboards. This behavior is seen on custom layouts when using the ArcSight Console, and image dashboards when using ArcSight Web and ArcSight Command Center. To view these fields correctly, use the standard layout on ArcSight Console.
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-1088	If a regular or inline filter with the condition "Event Annotation Flags Is NOT NULL" is applied to an Active Channel, the Active Channel will not load all of the matching events. Workaround is to use the following two filters in AND condition. EventAnnotationFlags Is NOT NULL EventAnnotationFlags != 0

ArcSight Manager

Issue	Description
ESM-51070	Connector statistics file to be processed correctly on Managers other than the primary destination Manager. Related content such as the rule Connector Discovered or Updated will be impacted.
ESM-48068	After asset auto-creation, if the manager does not restart and the server.std.log shows a message about a "conflicting device with the same hostname/ipaddress <resource id>", then 2 assets have the same resourceId. This conflict has to be resolved before starting the manager.
ESM-47625	When exporting a case or other resource, the Creation Time is changed to the time of the export.
ESM-46699	Updating a Trend by refreshing it works only once. Thereafter, the trend does not refresh with updated information.

Issue	Description
ESM-37488	Exporting a large active list with 10 million entries, or exporting rules that use such active lists, results in an exception in the server.std.log file. Additionally, the Manager runs out of memory and automatically restarts itself. Workaround: Use the export format instead of the default format while exporting the rule or active list definition using an archive or a package.
ESM-30008	Installing an exported package from a bundle file occasionally results in the following error: Install Failed: Resource in broker is newer than modified resource. Workaround: Re-import the package.
NGS-14293	The current version of ESM API (ver. 1.0) returns big negative numbers for NULL database fields. Depending on field type that would be either -2147483648 (Integer.MIN_VALUE) or -9223372036854775808 (Long.MIN_VALUE). All such fields in returned Resource or Event representations should be treated as NULL fields.
NGS-12358	A package resource may become out of sync with the content that has been added to the package. To workaround, recreate the package.
NGS-9734	In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.
NGS-9733	When logging in to the ArcSight Console, you could get an error related to logging in to core services.
NGS-9596	Time zone configuration files could become corrupt and prevent CORR-Engine from starting. Recovery requires restoring the time zone related files from backup.
NGS-9503	There is a possibility that small segments of data in the CORR-Engine may become corrupted. If a query attempts to access data that has become corrupted, the query will skip the corrupted data and log an error message in the MySQL log. This enables MySQL to continue and return a result on the data that is not corrupted.
NGS-9109	An incorrect OID is provided for ArcSight SNMP Trap. Third party package causes the OID for a trap to be translated incorrectly.
NGS-8926	If there is a Forwarding Connector running between a source Manager and any destination, and a correlation event occurs on the source Manager, then the Forwarding Connector will forward the correlation event and its associated correlated events to the destination. However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database. As a result, if there is any correlation content on the source Manager looking for the value EventAnnotationFlags=correlated, the content will not be matched or triggered.

Issue	Description
NGS-4837	With certain long running queries, a deadlock might occur in the JDBC driver. You might notice decreased throughput. If you suspect this, request a thread dump through manage.jsp and determine if the end of the dump specifically indicates "deadlock." Workaround: If a deadlock does occur and is an issue for you, restart the Manager to resume normal operations.
NGS-3825	If the field size of an event exceeds 32 KB, that event does not get persisted.
NGS-3294	At very high EPS rates and with a very high number of annotated events, the source Manager cannot send base events to the destination Manager.
NGS-1937	The Archive tool occasionally fails to import entries into an active list due to transient errors. In such situations, you might not see any errors, but the list does not get populated. Workaround: Re-import the same package.
NGS-172	Base events are not automatically annotated after rules trigger. Workaround: Set logger.base-event-annotation.enabled=true in server.properties.

CORR-Engine

Issue	Description
NGS-14041	Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the "Ignore Case" option, which rely on the UPPER function.
NGS-11080	When offline event archives are restored to another system using the restorearchives command, the event annotations are not restored. The offline archives are not affected.

Issue	Description
NGS-4884	It is possible to get no query result when querying the ArcSight.events table from arcdt or from mysql. If this occurs, execute the SQL using the command arcsight arcdt by following the steps below: 1. Create a file such as 1.sql in /tmp/ containing this SQL: "select * from arcsight.events where arc_deviceHostName = 'host_name' limit 2;" 2. Run arcdt tool and pass the created SQL file as parameter: -f /tmp/1.sql and the specified time frame assuming you have events for this time frame: ./arcsight arcdt runsql -f /tmp/1.sql -type EndTime -ss <start time> -se <end time> Use start and end times in the form YYYY-MM-DD-HH-MM-SS-MSS-TZ, such as 2013-02-04-00-00-00-000-PST. (MSS is milliseconds.) More information about running this tool can be obtained by running tool with help option (arcsight arcdt help), or by referring to this command in the Administrator's Guide chapter, "Administrative Commands."
NGS-4790	To resolve a "database full" condition, you can free up space in the ArcSight System Storage Space by doing the following: 1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend. 2. Reduce the retention period of specific trends. By default, trends retain 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 the trend runs. 3. 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.

Command Center

Issue	Description
NGS-14311	While configuring an existing filter condition of a channel, if the condition is "true" only, remove the "true" condition first before adding any other conditions.
NGS-14231	Some events from the last selected bucket may not be part of visualization.
NGS-14230	Visualization of variable fields is not supported.

Issue	Description
NGS-13926	The stages available in the ArcSight Console Stage drop-down list do not always display in the ACC active channel. The stage "Follow-Up" is available in the ArcSight Console Annotation Stage drop-down list, but does not display in the Annotation Stage drop-down list in ACC active channel.
NGS-13895	Type values should be in upper case in the ArcSight Console; are shown in lower case.
NGS-13854	If you are using other than an English installation, some dashboard pages may not load in the ACC. You can still access these pages through the ArcSight Console.
NGS-12984	Channels in ACC do not support concentrator agent field.
NGS-12968	The new date field global variable will not display date value correctly in ACC dashboards. For example, create a variable of this type : Type Conversion -> Convert String to Date Use this variable in two data monitors and added these data monitors to a dashboard. In the dashboard, one of the data monitor displays the date format correctly, but the other data monitor shows it as a long number.
NGS-11143	In visualization user interface, when there is an attempt to investigate fields with no values, the condition is set incorrectly. As a result, channel does not show any events.
NGS-11051	Some channels can be resource intensive, such as those with a time range of an hour or so. If a channel takes a long time to load in a high-traffic environment, open it in the ArcSight Console. To view a resource-intensive channel in Command Center, narrow the time range to 5 - 10 minutes to reduce the event volume. For optimum performance in high traffic environment, limit open channels to 3 per browser, though limit for channels per browser is 10. Command Center can support up to 15 less intensive channels and between the ArcSight Console and ArcSight Command Center, limit open channels to 25. Between the ArcSight Console and Command Center, ESM can support up to 25 open channels.
NGS-10634	The condition summary might not display completely in the condition summary window.
NGS-10413	When there are several active channels open on a page, refreshing an active channel can cause the error message "An unexpected error occurred when contacting the server" and the channel is not refreshed.

Issue	Description
NGS-9379	If you logged in to ArcSight Command Center using the Chrome browser and viewed the dashboard: /All Dashboards/ArcSight Administration/ESM/HA Monitoring/ESM HA Status, the Current Primary doesn't show the column name label for the System IP address and system HostName fields. This issue has also happened with /All Query Viewers/ArcSight Administration/ESM/HA Monitoring/System Status Changes. This issue did not happen with the Internet Explorer 11 or Firefox 24 ESR browsers or on the ArcSight console.
NGS-9358	If you log in to ArcSight Command Center and view the dashboard: /All Dashboards/ArcSight Administration/ESM/Event Analysis Overview/Event Count History, the page is blank and the Command Center continues to show "Loading...."
NGS-7907	When user perform peer search using IN operators for IP address, MAC address, or Enum fields, no results are returned and an error message is displayed. Workaround: None at this time.
NGS-7891	In Command Center Search, queries using some operators, such as chart, eval, rename, replace, rex, and regex, may not return the correct results when searching the following types of fields. IPv4 fields such as sourceAddress, MAC address fields such as destinationMacAddress, IPv6 fields such as dvc_custom_ipv6_address1, Geo Location fields such as: dest_geo_ latitude, as well as the agentSeverity and locality fields. For example the following queries may not return the correct results: ... | chart max(agentSeverity) by name ... | chart max(dest_geo_longitude) by name ... | replace Low with notToWorry in agentSeverity ... | replace Local with localevents in locality Workaround: None at this time.
NGS-7594	In the ArcSight Command Center, if you search by Load a Save Search filter, when the session times out, if you click the "Save current search filter" icon or "Load a save search filter" icon, you get logged out without a way to log back in. Workaround: When you see this behavior, close the browser window, reopen it, and log in to ArcSight Command Center again and continue with the search.
NGS-7584	A condition in a Case Query Group with owner = <username> will return an error while viewing cases of a case query group in any UI. Workaround: Use owner = <user resource_id> instead of owner = username.

Issue	Description
NGS-7518	In a Safari browser on a Mac OS, the search results page my not include a horizontal scroll bar. Workaround: Resize the browser to get the horizontal scroll bar.
NGS-7489	The session time out does not occur while the home page is loaded. If leaving a session unattended for an extended period, make sure you log out.
NGS-7315	If you delete a permission and then re-add the same permission and save it, the added permission is NOT saved. Workaround: After deleting a permission, save before re-adding or adding any permissions.
NGS-6896	In the Chrome browser, the Select Resource drop-down sometimes doesn't work properly. Workaround: If this occurs, refresh the page to restore the content. Alternatively, use another browser.
NGS-6805	When using the Chrome browser, the drop down to edit the Notification State or Storage Mapping might remain displayed when you move somewhere else by clicking outside the drop-down. Workaround: Click inside the drop-down and then click outside of it again to cause it to be removed from display.
NGS-6668	When report output is loading and you run another report, the current report is canceled and new report output is displayed. Workaround: Wait until the report output finishes loading before running another report.
NGS-5888	The Push History is only shown for subscribers that are online. If a peer is not online, the Push Status field in the Push History will be blank.
NGS-1283	Non-admin users cannot access the Users, Connectors, and Configuration page in ArcSight Command Center, even when provided with the permissions to do so. Workaround: You must have administrator privileges to access the Users, Connectors, and Configuration page in ArcSight Command Center.

Connectors

Issue	Description
NGS-12742	Event ID may appear as negative when using three or more forwarding connectors to a single destination. This can be ignored. A negative event can result because Java has only a signed 64 bit value, and in a multi-tier deployment that uses the higher 16 bit, event IDs may be presented as negative. For details, see the Event ID and Event Forwarding document, located at https://protect724.hp.com/docs/DOC-12310.

Issue	Description
NGS-12407	Annotation flag indicating 'forwarded' may not get set when forwarding events from ESM 6.8.
NGS-2052	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. For updating existing assets, please make use of one of the following attributes to identify them: - An External ID, or - a resource ID, or - a URI
NGS-1423	Upgrading a connector, running on Windows, from the ArcSight Console will fail if any process is using the connector's "current" folder. Workaround: 1. Make sure there are no files in the connector's "current" folder open. 2. Start the connector by using Start > Programs > Connector Programs. Do not start the connectors using the "arcsight agents" command.

Installation and Upgrade

Issue	Description
ESM-40984	Before uninstalling any ArcSight package, certain tasks must be performed in sequence. 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.
NGS-10718	When you uninstall ESM Console from Mac OS X, the shortcut in dock gets left behind. Workaround: To remove the shortcut in the dock, restart your system. After the system restarts, the shortcut is deleted form the dock.
NGS-10606	During the installation of ESM Console on Mac OS X, you have an option to create a shortcut in the dock. However, after installation completes, you will see that this shortcut is not created. Workaround: To get the shortcut in the dock, restart your system. After the system restarts, the shortcut in the dock is visible.

Issue	Description
NGS-10524	On the Apple OS X Mavericks platform for Macintosh, the ArcSight Console installation can complete with a message that some errors occurred during the install. Check the install log. You can ignore the following error: Install JRE: /Applications/arcsight/ESM6.8c/console_24927/Console/current/UninstallerData/resource/jre Status: ERROR Additional Notes: ERROR - JRE Source does not exist
NGS-7497	Console installation on localized path is working in some Windows 7 machines when installed in a French name like "C:\d'enquête" but not in other Windows 7 machines. Workaround: Due to the inconsistent behavior in Windows 7 machines, use English filenames only in installation paths. French names in path may cause installation to fail in certain Windows 7 environments.
NGS-3962	In GUI installation mode, the installation process automatically invokes the Suite Installer and the Configuration Wizard in sequence. If the Configuration Wizard fails with an error message, the Suite Installer will still indicate that the Suite has been successfully installed. Workaround: Either manually re-launch the Configuration Wizard from a command line after fixing the issue or uninstall the Suite installation and start over again. Refer to the ESM Installation and Configuration Guide for the command to use and the clean-up steps.
NGS-3839	Occasionally, the First Boot Wizard may fail to proceed due to some errors. If this happens, terminate the process. After checking the logs and correcting the errors, follow the clean up instruction in the ESM Installation and Configuration Guide and re-launch the installer.
NGS-3814	If you reboot your system immediately after the First Boot Wizard completes, but before you run the setup_services.sh command as the "root" user, the machine may come back in an unstable state. Running the setup_services.sh command now may not be able to bring up all Arcsight services. Workaround: 1. Do not reboot without running the setup_serivces.sh command while logged in as the "root" user. 2. If you reboot without running the setup_services.sh command, run setup_services.sh, and then reboot again.
NGS-3322	Due to the timing of some components' start-up, there may be some harmless error messages in the log files such as: [FATAL][default.com.arcsight.logger.distributed.DirectConnection$ReadChannel][run] java.io.IOException: end of communication channel [FATAL][default.com.arcsight.logger.distributed.ClientDirectConnection][run] java.nio.channels.ClosedChannelException

Management Console

Issue	Description
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.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (ESM Express 6.9.0c)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!