

Release Notes

ArcSight ESM 6.8c

January 29, 2015



Copyright © 2015 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>

Contact Information

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

Revision History

Date	Product Version	Description
01/29/2015	HP ArcSight ESM 6.8c	Release Notes

Contents

ArcSight ESM 6.8c	5
Welcome to ESM 6.8c	5
What's New in This Release	6
Beta Feature: Superindexes	9
Verifying the Downloaded Installation or Upgrade Software	9
Upgrade Support	10
Upgrade From ESM 6.0c Patch 3 or ESM 6.5c SP1	10
Migrating from ESM 5.x to ESM 6.8c	10
Geographical Information Update	10
Vulnerability Updates	11
Supported Versions for Distributed Searches	11
Supported Versions for Content Management	11
Supported Platforms	11
Supported Languages	11
Verifying Secure Delivery	12
Usage Notes	12
FIPS	12
Asset Model Import FlexConnector	12
Forwarding Connector	12
Domains	12
Running Concurrent Searches	12
Starting and Stopping Components	13
Issue When Subscriber is Added As a Peer	13
Scroll Bar Issues with Google Chrome and Apple Safari	13
ArcSight Web Issues with Internet Explorer 11	13
Using IdentityView 2.51 User Activity Profile	13
Trend Tables	13
Risk Insight Upgrade to 1.0.1	14
Localization	14
Open Channels in the Arcsight Command Center	14
Fixed Issues	14
Analytics	14
ArcSight Console	15
ArcSight Manager	16

CORR-Engine	17
Command Center	17
Connectors	17
Installation and Upgrade	18
Open Issues	18
Analytics	18
Analyze/Search	19
ArcSight Console	19
ArcSight Manager	23
CORR-Engine	25
Command Center	25
Configuration	29
Connectors	29
Installation and Upgrade	30
Localization	32

ArcSight ESM 6.8c

These release notes discuss the following topics.

- ["Welcome to ESM 6.8c" on page 5](#)
- ["What's New in This Release" on page 6](#)
- ["Beta Feature: Superindexes" on page 9](#)
- ["Verifying the Downloaded Installation or Upgrade Software" on page 9](#)
- ["Upgrade Support" on page 10](#)
- ["Geographical Information Update" on page 10](#)
- ["Vulnerability Updates" on page 11](#)
- ["Supported Versions for Distributed Searches" on page 11](#)
- ["Supported Versions for Content Management" on page 11](#)
- ["Supported Platforms" on page 11](#)
- ["Supported Languages" on page 11](#)
- ["Verifying Secure Delivery" on page 12](#)
- ["Usage Notes" on page 12](#)
- ["Fixed Issues" on page 14](#)
- ["Open Issues" on page 18](#)

Welcome to ESM 6.8c

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.

ESM 6.8c does not support FIPS.

What's New in This Release

This topic describes the new features and enhancements added in ESM 6.8c.



Active Channels in the ArcSight Command Center

You can now select channels to view events in the ArcSight Command Center. Each channel includes the channel summary, radar, and events displayed on the grid. Perform event annotation and view event priority statistics. You can also attach events to existing cases.

Select up to four fields and visualize data on the grid in an event chart and associated Top N chart per field. When you make further selections on the event chart, the Command Center employs unique filtering techniques to adjust or update the related charts based on your selection.

Refer to the following topics in the *ArcSight Command Center User's Guide's* section on "Monitoring Events Through an Active Channel."



Storage to 12 TB

Storage capacity is designed for up to 12 TB.



Correlation Enhancements

Automated optimization of rule and event data monitor conditions

You can now have ESM evaluate your rule and event data monitor conditions, then change the order of these conditions in memory to optimize the use of system resources.

While rules and data monitor filters don't have to be edited to benefit from this in-memory optimization, you can optionally change the conditions in rules and data monitors themselves. You do this by referring to the tracing information to re-order the conditions.

For information, refer to the following topics in the ArcSight Console User's Guide:

- ◆ "Optimizing the Evaluation of Conditions" in the Rules Authoring section
- ◆ "Optimizing the Evaluation of Data Monitors' Event Filters" in the Using Data Monitors section

New variable functions

- ◆ `GetCurrentTime` is available under the Timestamp category. Use it to provide current values similar to `$NOW`.
- ◆ The following list functions: `DistinctListValues`, `ListIntersection`, `ListUnion`, `NonNullListValues`, and `SortListValues`, are available under the Value List category. Use these functions to compare list values to values from a multi-mapped list.
- ◆ `ConvertResourceToReference` is available under the Type Conversion category. Create a variable with this function, then in your rule action to add an asset to an active list, select the asset as resource reference subtype.
- ◆ `FormatGroupOf`, `FormatGroupsOf`, `GetGroupOf`, and `GetGroupsOf` are now available for queries on active lists of assets or zones.

Refer to the ArcSight Console User's Guide for information on the above.

Rule actions on unique aggregation fields

Previously, in rules, you could only apply the rule actions `Set Event Field`, `Add to Active List`, and `Add to Session List` on identical aggregation fields. In this release, you can now use these actions on unique aggregation fields. Note that the `Set Event Field` action works on string fields only, using an expression in the format `@<fieldname>`.

Refer to "Rule Actions Reference" in the Rules Authoring section of the *ArcSight Console User's Guide*.



Pattern Discovery Enhancement

The Pattern Discovery feature has been enhanced to improve query performance when large datasets cause query problems. The optimization applies if, in a Pattern Discovery Profile, options under Advanced (Record Time Order and Split On Inactivity) are not checked.

Pattern Discovery is part of the Threat Detector solution package, a licensed feature. Refer to the section on Pattern Discovery in the *ArcSight Console User's Guide* for more details.



ESM Service Layer APIs

The following interfaces in the ESM Service Layer are officially supported:

- 1 CaseService
- 2 GroupService
- 3 LoginService
- 4 ResourceService
- 5 SecurityEventService
- 6 UserResourceService

The above Web services APIs are certified for REST applications in this release. Developers creating SOAP-based Java applications can also access the SDK libraries for core and manager services.

To get started, learn about the overall architecture, and view selected code samples, see the ESM Service Layer Developer's Guide. This guide also provides instructions on how to access the SDK libraries and Javadocs. The Javadocs contain detailed descriptions of the interfaces, methods, and parameters. The Javadocs are available as HTML (with the ESM installation) and as PDFs. Download the Service Layer Guide and Javadoc PDFs from Protect 724 at <https://protect724.hp.com/welcome>.



New Standard Content

- High Availability (HA) Monitoring lets you monitor the status of ESM systems that are using the optional [ESM High Availability Module](#).
- ArcSight ESM Device Monitoring enables you to monitor device status continuously with minimal impact on the ESM system.
- The Sortable Rule Stats data monitor in the Rules Status dashboard shows statistics for rule performance, such as partial matches, matching events, correlation events, time to execute, and memory used by each rule. This feature works only for standard and lightweight rules. You can sort the information in each column by clicking the column title.
- ArcSight System content now provides a new ArcSight Networks package that contains zones. In previous releases zones were included in the ArcSight Core package.

See the *ArcSight Core Security*, *ArcSight Administration*, and *ArcSight System Standard Content Guide* for information on standard content.

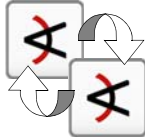


Package Format for Content Management

A new package format, **contentsync**, is available. Use this format when creating packages specifically for synchronizing content among the ArcSight Manager publisher and Manager subscribers.

For information on packages, refer to the *ArcSight Console User's Guide*.

For information on ESM peers and content management, refer to the *ArcSight Command Center User's Guide*.



ESM High Availability Module

The ESM High Availability Module (HA Module) is a separately-licensed feature that provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.

One ESM runs on the primary machine and selected hard-disk writes are mirrored to the secondary machine. The HA Module fails over to the secondary ESM which then becomes the primary ESM. During the failover, events are cached at the connectors, so that no data is lost.

For information, refer to the *ESM High Availability Module User's Guide*.



Automatic Base Event Forwarding

The Forwarding Connector for ESM 6.8c has been enhanced so that correlated base events are automatically forwarded to the destination Manager, along with the correlation events. You also have the option to turn off automatic base event forwarding and only pull correlated events into the destination Manager upon demand.

Refer to the *Forwarding Connector User's Guide* for instructions on how to set up ESM for automatic or on-demand base event forwarding.

Beta Feature: Superindexes

Superindexes is a feature available to qualified customers on a test basis in ESM 6.8c. 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.

Verifying the Downloaded Installation or Upgrade Software

HP provides code signing to enable you to verify that the software you have received to use for installation or upgrade is indeed from HP and has not been manipulated in any way by a third party. To do this, the software has been signed with a digital private key only held by HP.

Access the following link to download HP's public certificate:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

This site also provides the step-by-step instructions for how to import HP's public certificate and verify the signature file.

Upgrade Support

Direct upgrade to ESM 6.8c is supported from ESM 6.0c Patch 3 or 6.5c SP1. However ESM 6.8c does not support FIPS.

Upgrade From ESM 6.0c Patch 3 or ESM 6.5c SP1

Refer to the ESM 6.8c Upgrade Guide for instructions on how to upgrade your ESM 6.0c Patch 3 or ESM 6.5c SP1 installation to ESM 6.8c.

Migrating from ESM 5.x to ESM 6.8c

This release of ESM does not support a direct upgrade path from your ESM 5.x installations to ESM 6.8c. The supported paths are as follows:

From ESM 5.2, migrate to ESM 6.0c Patch 3, then upgrade to ESM 6.8c

From ESM 5.5, migrate to ESM 6.5c SP1, then upgrade to ESM 6.8c.

Do the following in the order listed below:

- 1 Install ESM 6.0c Patch 3 or ESM 6.5c SP1 (depending on the path you are taking, above) on a machine other than your existing ESM 5.x installation machine. Refer to the appropriate Installation and Configuration Guide for detailed steps to do so.

Do not make any changes to resources on this new installation; the migration will wipe them out.

- 2 Use the Resource Migration tool to migrate your resources from your existing 5.x ESM (effectively from the underlying Oracle database) to the newly-installed ESM 6.0c Patch 3 or 6.5c SP1.

The resource migration tool migrates only resources. It does not migrate event data. Keep your existing ESM instance running to maintain historical event data according to your retention policies.

Contact your HP Account Representative, if you plan to migrate your resources from your ESM 5.x installation, to discuss your requirements and coordinate migration.

The Resource Migration Tool is available for download from My Software Updates at <http://softwaresupport.hp.com>. Select the ArcSight ESM 6.8 product, then download the corresponding Resource Migration Tool from the Downloads list. Also, get the document, Migrating ESM Resources From Oracle to CORR-Engine and follow the detailed steps.

- 3 Upgrade to ESM 6.8c. Refer to the ESM 6.8c Upgrade Guide for detailed instructions.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20141001.

Vulnerability Updates

This release includes recent vulnerability mappings from the October 2014 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU-1187 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, MSKB
Enterasys Dragon IDS updated	Faultline, CVE, Nessus
Cisco Secure IDS S828 updated	Faultline, Bugtraq, CVE, X-Force, Nessus
Juniper / Netscreen IDP update 2429 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, MSSB, CERT
TippingPoint UnityOne DV8618 updated	Faultline, Bugtraq, CVE, Nessus
ISS SiteProtector updated	Bugtraq, CVE, X-Force, CERT

Supported Versions for Distributed Searches

Distributed searches are supported from ESM 6.8c to the following versions of ESM and Logger peers:

- ESM 6.8c
- ESM 6.5c SP1
- ESM 6.5c
- Logger 6.0
- Logger 5.5

For more information about distributed searches, look at the ArcSight Command Center User's Guide topic "About Searching for Events > Searching for Events > Searching Peers (Distributed Search)."

Supported Versions for Content Management

For this release, content management (synchronization) requires that all ESM Versions must be the same, including service packs and patches.

For more information about distributed searches, look at the ArcSight Command Center User's Guide topic "Administration > Content Management."

Supported Platforms

See the Consolidated Support Matrix document available on the Protect 724 site for details on ESM 6.8c platform and browser support.

Supported Languages

These languages are supported by ESM:

- English
- French
- Japanese

- Simplified Chinese
- Traditional Chinese
- Korean
- Russian

Korean and Russian language support has been added for ESM 6.8c.

Verifying Secure Delivery

To ensure that files have not been either corrupted or tampered with in transit, HP provides an MD5 cryptographic hash for each product component and documentation file.

To verify a software file from the product download site, do the following:

- 1 On the product file download page, select the file you want to download.
- 2 In the “Selected media product information” section, find the 32-digit MD5 signature.
- 3 Verify the MD5 checksum using an independently generated MD5 checksum of the file.

Usage Notes

FIPS

ESM does not support FIPS in this release.

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.

Forwarding Connector

Make note of the following for the ArcSight Forwarding Connector for ESM 6.8c:

- ESM 6.8c supports upgrading to Forwarding Connector 7.0.7.7286.0 from the previous Forwarding Connector release 6.0.4.6830.0 and 7.0.1.6992. If you are installing ESM 6.8c in a hierarchical environment, please install Forwarding Connector 7.0.7.7286.0 directly.
- If you are forwarding events from ESM 5.5 or ESM6.0c Patch 3, the Forwarding Connector version used must be the one released with the latest ESM version, in this case version 7.0.7.7286.0.
- See the Consolidated Support Matrix document available on the Protect 724 site for details on Forwarding Connector 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.

Starting and Stopping Components



The commands for starting and stopping components in ESM 6.8c are different than the commands for starting and stopping components that were used in prior releases of ESM with Oracle backend.

Also, in ESM 6.8c, the commands for starting and stopping components should be run as user *arcsight*.

Running unsupported scripts may produce unexpected results, including system failure or data loss.

For help on the `arcsight_services` command supported scripts, enter the following:

```
/etc/init.d/arcsight_services help
```

If you inadvertently run unsupported scripts, rebooting the system will restore proper operation in most cases.

Issue When Subscriber is Added As a Peer

An error message is shown for manual pushes that are attempted if there are no enabled subscribers. However, no similar error message is displayed for automatically scheduled pushes if there are no enabled subscribers.

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.

ArcSight Web Issues with Internet Explorer 11

ArcSight Web has two issues with Internet Explorer 11:

- On the Dashboard page, if you choose one dashboard and click "Edit Layout," then try to drag and drop to edit dashboard layout, it does not work.
- From Reports > Archived Reports, if you when you click the download icon for a report the downloaded report name is changed to "app" and the format is not correct.

Using IdentityView 2.51 User Activity Profile

The IdentityView 2.51 profile called `/All Profiles/ArcSight Solutions/IdentityView 2.5/User Activity Monitoring/User Activity - Differing Attacker and Target Usernames` should be de-activated or the time range changed to a one-hour interval. This profile has a high runtime overhead. It is looking for events over an entire week, which can be large, and then looking for patterns of length 2. If allowed to run in real time, it can cause the machine to run out of memory.

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.

Risk Insight Upgrade to 1.0.1

To use ArcSight Risk Insight with ESM 6.8c, you must apply the Risk Insight 1.0.1 patch to upgrade Risk Insight 1.0 to 1.0.1. See the ArcSight Risk Insight Release Notes for details.

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 is 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.

Fixed Issues

Analytics

Issue	Description
NGS-9501	Partial matches on events were reported for lightweight rules, even if these do not apply because lightweight rules execute actions on every event. This was fixed in code. You should no longer see partial matches on lightweight rules.
NGS-8839	In a Query, the <code>GetHour</code> variable returned the hour translated from local time to GMT. For example, if your local time is 20:31:47, the <code>GetHour</code> variable might return 3, instead of 20, as expected. This issue is now fixed.
NGS-8831	If you queried cases with the condition, <code>Owner = <the user's name></code> , the query failed because it was expecting the owner's Resource ID. This issue is now fixed. Now, if you query a case for the owner, you can either use the owner's Resource ID or the owner's name.
NGS-8684	In certain scenarios, active list updates were not occurring even though audit events indicate that such updates were successful. This issue is now fixed.

Issue	Description
NGS-8682	<p>In some instances, when an ActiveList was modified at a high rate, the ActiveList cache would become inconsistent with the underlying database table, with the table row count exceeding the configured list capacity. As a result of this inconsistency, updates to entries not found in the cache were sent to the database as INSERT operations, resulting in a CONSTRAINT VIOLATION exception due to the entry being present in the database table. In addition, multiple ActiveList tables were updated in the same database transaction, causing the exception in one ActiveList to roll back updates that had previously been made in other ActiveLists.</p> <p>This issue is now fixed.</p>
NGS-8681	<p>In some cases, in drilldowns where Concatenate(NULL, NULL) returned an empty string, i.e., "", and ToLower(NULL) returned NULL, where NULL is a null value. This issue has been fixed. After the fix, a variable constructed from Concatenate(NULL, NULL) will return NULL, and a variable constructed from ToLower(NULL) will return NULL as well.</p>
NGS-8578	<p>Event throughput would sometimes drop significantly after the Manager had been running for a period of 1-2 weeks, for no obvious reason. This was happening due to the CodeCache (a section of the JVM heap used by the just-in-time compiler) becoming full.</p> <p>The problem has been fixed by increasing the CodeCache capacity setting.</p>
NGS-8457	<p>There were several cases where there were no functions to compare lists from events to a list returned from a multi-mapped active list. As a result five new list functions have been added under the Value List category and are documented in the ArcSight Console User Guide:</p> <ol style="list-style-type: none"> 1. DistinctListValues 2. ListIntersection 3. ListUnion 4. NonNullListValues 5. SortListValues
NGS-8160	<p>A translation performed by the Console for GetDayOfWeek was not performed in the same way on the Manager. This issue is now fixed. One part of the fix is from the UI. A second part of fix is changing the mapping in an active list such that Sunday is mapped to 1, Monday is mapped to 2, ..., and Saturday is mapped to 7 when using the GetDayOfWeek function.</p>

ArcSight Console

Issue	Description
NGS-10673	<p>If you open a Query Viewer, adjusted the column widths, and then clicked Refresh, the column widths would return to default size.</p> <p>We have improved this functionality so that the column widths remain as changed until the ArcSight Console session is closed. (When you log in again the defaults are restored.)</p> <p>Note that if you click Refresh repeatedly and rapidly enough, the Query Viewer columns will return to the default widths.</p>

Issue	Description
NGS-9985	Active channel loaded slowly when a request URL file name was used in the active channel filter. This issue is now fixed.
NGS-9755	Using a case condition in a search group for "Conclusion is NULL" failed. This issue is now fixed.
NGS-9597	For the same trend parameters, the duration displayed in the Data Viewer was different between ESM 5.2 and ESM 6.5. This issue is now fixed.
NGS-9590	Generator URI field (group by) value was truncated in Query Viewer. This issue is now fixed.
NGS-9581	If an active channel that uses a field set was copied into a non-admin active channel folder, an error was generated. This issue is now fixed.
NGS-9464	A resource change in ESM Console generated an ArcSight internal event with some missing user information. The event fields Target User Name and Target User ID were empty. This issue has been fixed.
NGS-9077	If rules were moved and when they were fired, the GeneratorURI path listed the original location of the rule rather than the current location of the rule. This is now fixed.
NGS-9058	Changes to a connector filter were remaining local and were not made available across all connectors. This issue has been fixed.
NGS-8904	In SetEventField Rule action, the user was unable to select fields of type Zone. This issue is now fixed, these fields are evaluated if they are added to Identical Aggregation.
NGS-8347	HOURL and MINUTE functions were not working properly in reports. This issue is now fixed.
NGS-7526	Non-admin users under Default User Group did not have read permission to /All Trends/ArcSight Core Security, but this has been fixed so they have read access.
NGS-4091	If the arc_notification_history and arc_notification_registry were large, the ArcSight Console would hang. The system now allows users to log in even if the history and registry tables are large. This issue is now fixed.

ArcSight Manager

Issue	Description
NGS-8980	If the active list entries in database were significantly more than the configured capacity of the active list, in some cases, server startup may not be successful. This issue is now fixed.

Issue	Description
NGS-8680	<p>In a rule condition where request URL Host or Destination Host Name was identified as null were still processed though rule conditions were defined otherwise.</p> <p>This issue is now fixed.</p> <p>isNOTNULL however NULL events are still triggering the Condition</p>
NGS-8640	<p>NullPointerExceptions were written to log files due to a missing DeviceCustomString4 field value in Audit events received from connectors.</p> <p>This issue is now fixed.</p>
NGS-7580	<p>In Content Management, when running multiple package operations at the same time (both manual and scheduled operations), occasionally, one of the operations might fail due to a database deadlock.</p> <p>Now, the system detects this deadlock and gives a message that it could not perform the action because the package framework is locked, and asks you to try again later.</p>

CORR-Engine

Issue	Description
NGS-9592	<p>In some installations of ESM 6.0c and onward, annotation creation can be seen to occur slowly, on the order of 1-3 events annotated per second after pressing OK in the annotation dialog in the ArcSight ESM Console. This issue is more likely to occur if there are several active channels open simultaneously, as these other channels will push the events to be annotated out of the event cache in the manager service. Without this fix, if the events to be annotated are not present in the event cache, they are fetched one-at-a-time from the logger backend.</p> <p>With this fix, the events are fetched in larger batches to improve efficiency and reduce the overall time taken to annotate the events.</p>
NGS-8319	<p>Filters using Target and Attacker User Name fields were not working as expected in active channels or reports when used with ignore case.</p> <p>This issue has been fixed.</p>

Command Center

Issue	Description
NGS-10510	<p>The ArcSight Command Center User's Guide now provides the location of the log file pertaining to peer configuration.</p>

Connectors

Issue	Description
NGS-9561	<p>The Forwarding Connector Configuration Guide now contains clarified information regarding the Correlation Forwarding Connector.</p> <p>This issue is now fixed.</p>

Issue	Description
NGS-4900	The forwarding connector now forwards correlated base events along with the correlation events. See the Forwarding Connector Configuration Guide for details.

Installation and Upgrade

Issue	Description
NGS-10757	Upgrade failed due to 1-hour timeout setting on the system tables export. This issue is now fixed.
NGS-9346	Previously, when installing an upgrade or a patch, you could sometimes run out of JVM memory. This issue is now fixed.
NGS-8338	If you customized the file <code>/opt/arcsight/logger/data/mysql/my.cnf</code> , then before you upgrade, the changes you made are saved in a file called <code>my.cnf.sug</code> automatically during the upgrade. After the upgrade, restore your customizations from the backed up copy of the file.
NGS-5295	Previously, the upgrade script assumed that the password for both ArcSight and MySQL were the same password. This issue is now fixed and these passwords can be different.

Open Issues

Analytics

Issue	Description
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 <code>//</code> (double slash) and <code>/</code> (single slash); or within <code>//</code> (double slash) and <code>:</code> (colon). For example: :8443">https://&lt;hostname>: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.

Issue	Description
NGS-10374	When exporting events from the Case Details channel, archived events are not exported.
NGS-10244	The Sortable Rule Stats dashboard currently does not include information for pre-persistence rules.
NGS-9629	The Trend table stores only a single element for group variables (GetGroupsofAsset or FormatGroupsofAsset). This occurs when a trend contains any field made of such a group variable. This behavior occurs because Trends do not support the list data type internally. There is no workaround yet for this issue.
NGS-9376	Rule actions on unique aggregation fields (new feature) does not work with the rule trigger "On Time Window Expiration" when rule chain is on.
NGS-7896	Some rules under /All Rules/ArcSight Core Security can get triggered twice, because they are linked to other packages (for example, when the Intrusion Monitoring Foundation is installed). Workaround: Remove one of the links from the Real-Time Rules group.
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.
NGS-6509	If you have the IdentityView 2.5 solution and have 500 K actors, the actor channels are not being loaded. This happens intermittently.
NGS-5756	From within a Query Viewer drill down for Active Channel, you cannot drill down to Field Set having IP address as part of Global Variable.

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 Logger 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-50470	The filter (Source FQDN Is NOT "") does not work on Active Channels.
ESM-50373	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.

Issue	Description
ESM-41019	<p>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.</p> <p>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.</p>
ESM-40587	<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	<p>The Console can become unresponsive if you access other resources while building category models with a large number of actors.</p>
ESM-39829	<p>Deleting actors will require category models, if any, to be re-built. Each rebuild should only take a few seconds. However, when thousands of actors are deleted, the cumulative deletion period may last for hours.</p>
ESM-39331	<p>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.</p> <p>Workaround: To view additional fields in an Actor channel, add the fields to an Actor field set and use it in the actor channel.</p>
ESM-37344	<p>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.</p> <p>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.</p>
ESM-36055	<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, no error will be displayed indicating that you are not able to view some resources in the query due to lack of sufficient permissions.</p>
NGS-11212	<p>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.</p>
NGS-11153	<p>The console starts up successfully, but with the error message</p> <p>iCannot find sree properties in /home/arcsight/Console/current/reports/sree.properties."</p> <p>Workaround: Ignore this message.</p>
NGS-10819	<p>Some rules in the Intrusion Monitoring package with 1 day interval might fail in the very high EPS environment.</p> <p>Workaround: Change the Trend Interval to 1 hour.</p>
NGS-10679	<p>In the Macintosh 10.9 environment, event details are not displayed in the Inspect/Edit panel when an event is double-clicked. Workaround: use another browser.</p>
NGS-10208	<p>Not all listed resources are translated for the Korean locale.</p>

Issue	Description
NGS-9869	<p>Some local variables do not display in active channels if they have global variable fields as parameters. This is an existing issue with local variables, which will be fixed in a later release.</p> <p>The workaround is to do one of two things:</p> <p>a) Don't use a local variable for this, use a global variable instead or</p> <p>b) create an alias local variable that aliases the local variable, and use the alias variable in the FieldSet</p>
NGS-9640	<p>Previously CAC software used to pop up its own dialog to enter a PIN. Now with the fix, the ArcSight Console shows a dialog to enter a PIN when the user clicks the PKC11 login button to authenticate.</p>
NGS-9520	<p>If a customer opened a Query Viewer, adjusted the column widths, and then clicked Refresh, the column widths would return to default size.</p> <p>We have improved this functionality so that the column widths remain as changed until the ArcSight Console session is closed. (When you log in again the defaults are restored.)</p> <p>Note that if the user clicks Refresh repeatedly and rapidly enough, the Query Viewer columns will return to the default widths.</p>
NGS-9057	<p>Some standard content rules may impact system performance in certain customer environments. To identify resource-intensive rules, open the dashboard /All Dashboards/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status, and disable resource-intensive rules.</p>
NGS-8630	<p>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.</p> <p>In that case, the query viewer must be viewed in a table.</p>
NGS-8283	<p>When the time zone is set as a non-Default Time Zone (for example, Device Time Zone), and is in a time zone using Daylight Saving Time, some time functions, such as getHourOfDay, will return timestamps with a one hour offset to the actual hour. Functions return the correct hour value in timestamps that occur during standard time.</p>
NGS-8153	<p>When the regional language of the operating system is Simplified Chinese, some characters do not display as Chinese characters, but as English alphabet characters instead.</p>
NGS-8025	<p>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.</p>
NGS-7735	<p>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.</p>
NGS-7173	<p>The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.</p>
NGS-5981	<p>When selecting a group of events in a channel (for example, 500-1000 events) and marking them reviewed, not all events are annotated.</p>

Issue	Description
NGS-5975	If you are accessing query viewers with actor content, and you have a large number of actors, there may be a pause in the user interface while it waits for data from the Manager. This could result in a delay of several seconds.
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-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-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-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 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
NGS-146	In some cases, event-based Active Channels that include an InCase filtering condition do 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. Case-related events are copied to a special table so they can remain available after being archived, but the channel is unable to find and display such events correctly after the partition is archived. Workaround: Use the case event editor or Reports, which can correctly find and display these events.

ArcSight Manager

Issue	Description
ESM-51070	<p>When you add a new connector and specify a second destination that is an ESM, the active list "Connector Information" on the second-destination ESM will contain incomplete or incorrect information.</p> <p>Ignore the active list "Connector Information" on the second-destination ESM until the issue is fixed.</p>
ESM-48543	<p>When exporting user resources in a Package, the Running Reports folder fails to be included, and will not be created when the package is imported. There is currently no workaround for this issue.</p>
ESM-47625	<p>When exporting a case or other resource, the Creation Time is changed to the time of the export.</p>
ESM-46699	<p>Updating a Trend by refreshing it works only once. Thereafter, the trend does not refresh with updated information.</p>
ESM-37488	<p>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.</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-30008	<p>Installing an exported package from a bundle file occasionally results in the following error:</p> <p>Install Failed: Resource in broker is newer than modified resource.</p> <p>Workaround: Re-import the package.</p>
NGS-11097	<p>Running the High Availability First Boot Wizard to install HA software on a new secondary may take a long time - sometimes over 20 minutes.</p>
NGS-10306	<p>In a High Availability cluster If the number of connected hosts (N), and the ping timeout (T) entered into the First Boot Wizard are both large - in particular when:</p> $(N + 1) * T > 20$ <p>the cluster will never detect a network communication problem to the primary, and failover.</p> <p>Workaround: Use the Cluster Parameters Wizard to reduce N and T so that $(N + 1) * T < 20$. This will allow the secondary to automatically take over when the primary has been disconnected from the rest of the network.</p>
NGS-9734	<p>In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.</p>
NGS-9733	<p>When logging in to the ArcSight Console, you could get an error related to logging in to core services.</p>
NGS-9596	<p>ESM was not able to start because of corruption of time zone files.</p>
NGS-9503	<p>An attempt to access corrupt data in the CORR-Engine caused MySQL to become unresponsive. The issue has been addressed by skipping the corrupt data and logging an error message in the MySQL log. This enables MySQL to continue and return a result.</p>

Issue	Description
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-8573	<p>If case customization was done on the existing 6.x environment prior to 6.5c SP1 upgrade, the customizations are not copied over automatically during upgrade. It affects both manager and ArcSight Command Center.</p> <p>As a workaround, copy the following files which had customizations prior to upgrade to the current upgraded locations:</p> <ol style="list-style-type: none"> 1. Copy label_strings_en.properties and resource_strings_en.properties under /opt/arcSight/manager.preUpgradeBackup/i18n/common to /opt/arcSight/manager/i18n/common. <p>Note: For English, if the *_en.properties file does not exist under /opt/arcSight/manager.preUpgradeBackup/i18n/common, copy the *.properties file. If it exists, copy *_en.properties. For other locales, copy the *_{locale}.properties file.</p> <ol style="list-style-type: none"> 2. Copy caseui.xml under /opt/arcSight/manager.preUpgradeBackup/config to /opt/arcSight/manager/config. 3. If customized case details mapping to audit events exists, copy case.properties under /opt/arcSight/manager.preUpgradeBackup/config/audit to /opt/arcSight/manager/config/audit. <p>Restart the Manager for these changes to take effect.</p>
NGS-8285	<p>If services fail to stop after running "/etc/init.d/arcSight_service stop" or "/etc/init.d/arcSight_service stop all", you can stop them with</p> <p>/etc/init.d/arcSight_services killAllFast</p>
NGS-7790	If the ArcSight Command Center session expires while running Risk Insight, the Risk Insight session will also end. To restore the Risk Insight session, log back into the ArcSight Command Center.
NGS-6236	<p>Long reports might cause an OutOfMemoryError error in ESM processes.</p> <p>Workaround: If you expect a report to return a large amount of data, run the report when there is no other activity in ESM.</p>
NGS-4837	<p>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."</p> <p>Workaround: If a deadlock does occur and is an issue for you, restart the Manager to resume normal operations.</p>
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 too many annotated events, the source Manager cannot send base events to the destination Manager.
NGS-1937	<p>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.</p> <p>Workaround: Re-import the same package.</p>
NGS-1449	Shutting down services by using the arcSight_services command might result in exceptions in the log file. These exceptions are due to an issue with the order in which the components are shut down, and can be safely ignored.

Issue	Description
NGS-172	Base events are not automatically annotated after rules trigger. Workaround: Set <code>logger.base-event-annotation.enabled=true</code> in <code>server.properties</code> .

CORR-Engine

Issue	Description
NGS-11080	In a disaster-recovery scenario where event archives were restored onto a brand new, plain vanilla system, you could not restore annotations for event archives that were in the online state. This fix resolves that problem. The offline archives were unaffected.
NGS-4884	<p>If not done correctly, you might get no result querying the <code>ArcSight.events</code> table from <code>arcctl</code> or from <code>mysql</code>.</p> <p>Execute the SQL using the command <code>arcsight arcctl</code> by following the steps below:</p> <ol style="list-style-type: none"> 1. Create a file such as <code>1.sql</code> in <code>/tmp/</code> containing this SQL: <code>"select * from arcsight.events where arc_deviceHostName = 'host_name' limit 2;"</code> 2. Run <code>arcctl</code> tool and pass the created SQL file as param: <code>-f /tmp/1.sql</code> and the specified timeframe assuming you have events for this time frame: <code>./arcsight arcctl runsql -f /tmp/1.sql -type EndTime -ss <start time> -se <end time></code> <p>Use start and end times in the form <code>YYYY-MM-DD-HH-MM-SS-MSS-TZ</code>, such as <code>2013-02-04-00-00-00-000-PST</code>. (MSS is milliseconds.)</p> <p>More information about running this tool can be obtained by running tool with help option (<code>arcsight arcctl help</code>), or by referring to this command in the Administrator's Guide chapter, "Administrative Commands."</p>
NGS-4790	<p>To resolve a "database full" condition, you can free up space by doing the following:</p> <ol style="list-style-type: none"> 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 <code>"bin/arcsight dropSLPartitions -h"</code> 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-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.

Issue	Description
NGS-11051	<p>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 ñ 10 minutes to reduce the event volume.</p> <p>For optimum performance in high traffic environment, limit open channels to 3 per browser, though limit for channels per browser is 10.</p> <p>Command Center can support up to 15 less intensive channels and between the ArcSight Console and ArcSight Command Center, limit open channels to 25.</p> <p>Between the ArcSight Console and Command Center, ESM can support up to 25 open channels.</p>
NGS-10958	In the ArcSight Command Center, various pages are not translated for Korean locale.
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.
NGS-10140	Analyzer Administrator users may not be able to view actor-related content from the ArcSight Administration package. See the ESM Administrator's Guide in the sections "Permissions Required to Use Actor-Related Data" and "Granting or Removing Resource Permissions", and follow the steps to give the desired user group permissions for these resources.
NGS-9379	<p>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.</p> <p>This issue is also happened with /All Query Viewers/ArcSight Administration/ESM/HA Monitoring/System Status Changes.</p> <p>This issue did not happen with the I.E 11 or Firefox 24 ESR browsers or on the ArcSight console.</p>
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-9192	Condition summary can appear to differ between the ArcSight Console and the ArcSight Command Center. The values are not affected; what is different is the filter definition string. The filter definition should be parsed as shown in the ArcSight Console and will be fixed in the future.

Issue	Description
NGS-8733	<p>Currently the ArcSight Command Center search ignores events with a NULL value in the field you are searching for, unless you specifically add NULL values (IS NULL) to the search criteria. For example, searching for a sourceAddress that is NOT InSubnet would ignore NULL source Addresses.</p> <p>The workaround is either search them through the ArcSight Console or ArcSight Web, or change such a query in ArcSight Command Center to add the condition "sourceAddress IS NULL" and use "or" to concatenate the condition to the original condition.</p> <p>For example:</p> <p>NOT sourceAddress InSubnet "10.*.*.*"</p> <p>should be queried as:</p> <p>sourceAddress IS NULL OR NOT sourceAddress InSubnet "10.*.*.*"</p>
NGS-7907	<p>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.</p> <p>Workaround: None at this time.</p>
NGS-7891	<p>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.</p> <p>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.</p> <p>For example the following queries may not return the correct results:</p> <p>... chart max(agentSeverity) by name</p> <p>... chart max(dest_geo_longitude) by name</p> <p>... replace Low with notToWorry in agentSeverity</p> <p>... replace Local with localevents in locality</p> <p>Workaround: None at this time.</p>
NGS-7648	<p>The performance of peer search is slow in the current implementation.</p> <p>Workaround: None at this time. We will address this performance issue in future release.</p>
NGS-7594	<p>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.</p> <p>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.</p>
NGS-7584	<p>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.</p>
NGS-7570	<p>When running very large report from the Command Center, the Report view can become slow and possibly unresponsive as report is being downloaded for viewing.</p> <p>Workaround: Run a very large report from the ArcSight Console.</p>
NGS-7518	<p>In a Safari browser on a Mac OS, the search results page may not include a horizontal scroll bar.</p> <p>Workaround: Resize the browser to get the horizontal scroll bar.</p>
NGS-7489	<p>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.</p>

Issue	Description
NGS-7315	<p>If you delete a permission and then re-add the same permission and save it, the added permission is NOT saved.</p> <p>Workaround: After deleting a permission, save before re-adding or adding any permissions.</p>
NGS-7079	<p>If your environment contains more than 10,000 cases in one single group, displaying them in ArcSight Command Center might be very slow.</p> <p>Workaround: Avoid accumulating a large number of cases in one single group of your system. If your system contains more than 10,000 cases in one single group, display them in the ArcSight Console rather than Command Center.</p>
NGS-6896	<p>In the Chrome browser, the Select Resource drop-down sometimes doesn't work properly.</p> <p>Workaround: If this occurs, refresh the page to restore the content. Alternatively, use another browser.</p>
NGS-6886	<p>When a system has several peers and a peer stops responding, some pages in the ArcSight Command Center user interface might become slow to display. The delay happens regardless of the reason the peer system stopped responding.</p> <p>Workaround: Identify the peer that is not responding and remove its peer relationship on the Administration > Peers page, Peer Configuration tab. You can re-add the Peer later, when it is back in service.</p>
NGS-6812	<p>The ESM server log and the Logger server log may contain messages that say "...NotSerializableException: ...PeerLoggerRequestDestination".</p> <p>These messages do not indicate an active problem. You can ignore them.</p>
NGS-6805	<p>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.</p> <p>Workaround: Click inside the drop-down and then click outside of it again to cause it to be removed from display.</p>
NGS-6668	<p>When report output is loading and you run another report, the current report is cancelled and new report output is displayed.</p> <p>Workaround: Wait until the report output finishes loading before running another report.</p>
NGS-6634	Storage Group names are limited to contain only ASCII letters, digits and spaces.
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-3892	In the ArcSight Command Center, Dashboards that contain a Data Monitor of type 'System Monitor' or 'System Monitor Attribute' will display only the first 100 rows.
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.</p> <p>Workaround: To avoid this problem, set the refresh rate to a higher value. You can manually refresh the dashboard if needed.</p>
NGS-2301	<p>While the Dashboards you create in the ArcSight Console can have 3D bar charts, ArcSight Command Center does not support 3D bar charts.</p> <p>Workaround: To see 3D bar charts correctly, you need view them in the ArcSight Console.</p>

Issue	Description
NGS-1745	When viewing a Management Console dashboard in custom layout mode, such as "/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status", if the DataMonitors or Query Viewers overlap, click on Edit->Auto-Arrange to correctly display them. You can then save the arranged dashboard.
NGS-1582	In the Command Center'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. Workaround: Set the row limit of Query Viewers below 100 before viewing the dashboard in custom layout format.
NGS-1283	Non-admin users cannot access the Users, Connectors, & 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, & Configuration page in ArcSight Command Center.

Configuration

Issue	Description
NGS-10800	An error like the following will appear in the logger logs during logger startup: Caused by: java.io.IOException: /opt/arcsight/manager/bin/nss/linux64/libnssutil3.so: version `NSSUTIL_3.13' not found (required by /opt/arcsight/logger/current/local/nss/lib/libnss3.so) This will not cause any issue and can be safely ignored.

Connectors

Issue	Description
NGS-10788	Forwarding Connector supports FIPS but ESM 6.8c does not. So, you should not turn ON FIPS on the Forwarding Connector component though it can be enabled.
NGS-5137	Deleting hosts from the WUC host table results in the hosts below the deleted hosts being shifted up in the table. However, the eventpollcount setting for the shifted hosts is not shifted accordingly.
NGS-1423	On a Windows machine, upgrading a connector from the ArcSight Console will fail if any process is using the connector's "current" folder. Workaround: <ol style="list-style-type: none">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-49566	The Case schema customized settings are not transferred over during upgrade. Please contact Customer Support for help with transferring the Case customization settings.
ESM-41148	<p>During ESM upgrade, autozoning will fail if the number of assets in a zone/group exceeds 1000.</p> <p>Workaround: Manually run autozoning in batches of 1000 assets or fewer after completing your upgrade. You can do this from the Asset Channel or Asset Resource Tree in the Console.</p>
NGS-10524	<p>Installation errors can occur when installing the Console on the Apple OS X Mavericks 10.9.2 platform for Macintosh.</p> <p>Workaround: You can ignore these errors in the installation log.</p>
NGS-10147	After installing the ArcSight Core package, the package view may show some resources displayed in red strike-through text. These resources are purposely not included in the package and can be safely ignored.
NGS-9980	X11 must be configured on the machine before ESM Upgrade process is run. Otherwise, the upgrade will fail.
NGS-9752	<p>If the ESM destination is removed and reinstalled, then the ESM certificate needs to be removed manually from the trust store before it can get reimported again during the reinstallation and reestablish communication with the Forwarding Connector.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Export the certificate from the destination ESM 2. Add the certificate to the connector truststore manually. 3. Add the destination ESM via the wizard.
NGS-7497	<p>Console installation on localized path is working in some Windows 7 machines when installed in a French name like "C:\d'enqu&#xEA;te" but not in other Windows 7 machines.</p> <p>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.</p>
NGS-7274	<p>In this release, the generation of audit events for the Top Value Counts data monitor is disabled by default. This was enabled in a previous release (ESM 6.0c). If you upgraded to this release, you will not see those audit events.</p> <p>Workaround: If you want to continue seeing audit events for the Top Value Counts data monitor, log in to the ArcSight Console. Edit the Top Value Counts data monitor and select the Send Audit Events option.</p>
NGS-6996	There might be some data monitors disabled after the upgrade, while they are enabled in a fresh installation and vice versa. Workaround: re-enable any data monitors that you want enabled after upgrade.
NGS-5255	<p>As part of a resource migration and upgrade, if you perform the step to upgrade the Content, this error message is displayed:</p> <p>Error importing appliance post install archive</p> <p>To recover from this error, refer to the document, MigrateTo_CORRE.pdf, and see the Troubleshooting section.</p>

Issue	Description
NGS-3971	<p>When running the installer in console mode, make sure that X11 (X Windows) is NOT configured for the console. A X11 setup will cause the installation to abort with the following exception in the database.configuration.log file:</p> <pre>"java.lang.NoClassDefFoundError: Could not initialize class sun.awt.X11GraphicsEnvironment".</pre> <p>Should this happen, follow the clean-up instructions in the ESM Installation and Configuration Guide and re-launch the installer from a console that does not use X11 (X Windows).</p>
NGS-3962	<p>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.</p> <p>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.</p>
NGS-3871	<p>Under certain circumstances, the Uninstaller may not be able to remove all ESM 6.0c files under the /opt/arc sight/ directory. Refer to the Troubleshooting appendix in the ESM Installation and Configuration Guide on how to do the cleanup manually.</p>
NGS-3839	<p>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.</p>
NGS-3814	<p>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.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Do not reboot without running the setup_servics.sh command while logged in as the "root" user. 2. If you reboot without running the setup_services.sh command, uninstall and then re-install the product.
NGS-3808	<p>After you select "Next" on the "About to Configure ESM v6.5c" panel, if there is any failure, you will need to uninstall the product before you can reinstall it. Refer to the "Uninstalling ESM" section in ESM Installation and Configuration Guide.</p>
NGS-3445	<p>In some situations, the Installer panel may indicate that the installation was successful even though Web Server fails to start. Refer to the Administrator's Guide on how to manually configure and start the Web Server.</p>
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> <pre>[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</pre>
NGS-2783	<p>When a forwarding connector is installed, Superconnectors group is created under Custom Users Groups group. In addition, No Events enforcing filter is replaced by a specific event filter. After the upgrade, No Events enforcing filter will be reinstated meaning that no events will be forwarded from the Manager to the destination. The workaround is to remove the No Events enforcing filter.</p>

Localization

Issue	Description
NGS-4220	<p>In the Traditional Chinese localized environment, the Reports display code.</p> <p>Workaround:</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>