

# Release Notes

---

ArcSight ESM 6.5c

October 15, 2013



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

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

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

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

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

## Contact Information

---

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

---

## Revision History

---

<b>Date</b>	<b>Product Version</b>	<b>Description</b>
10/15/2013	HP ArcSight ESM 6.5c	Release Notes

---

# Contents

---

<b>ArcSight ESM 6.5c .....</b>	<b>5</b>
Welcome to ESM 6.5c .....	5
What's New in This Release .....	5
ArcSight Command Center .....	5
Rules .....	6
Lists .....	6
Reports .....	6
Cases .....	6
Actors .....	7
Saved Searches and Search Filters .....	7
Variable Functions .....	7
Event Priority Rating .....	7
Migration of ESM Resources from Oracle to CORR-Engine .....	8
ArcSight Risk Insight .....	8
Upgrade Support .....	8
Upgrade From ESM 6.0c .....	8
Migrating from ESM 5.x to ESM 6.5c .....	8
Geographical Information Update .....	9
Vulnerability Updates .....	9
Supported Platforms .....	9
ESM Patches .....	9
Verifying Secure Delivery .....	9
Usage Notes .....	10
Forwarding Connector .....	10
Domains .....	10
Browser Support in FIPS with Suite B Mode .....	10
Running Concurrent Searches .....	10
Starting and Stopping Components .....	10
Issue When Subscriber is Added As a Peer .....	11
Discover Fields List - Top Values and Values by Time .....	11
Frequently Asked Questions about ESM with CORR-Engine .....	11
Fixed Issues in ESM 6.5c .....	14
Analytics .....	14
ArcSight Console .....	14

---

ArcSight Manager .....	16
ArcSight Web .....	16
CORR-Engine .....	17
Open Issues in ESM 6.5c .....	17
Analytics .....	17
ArcSight Console .....	20
ArcSight Manager .....	23
CORR-Engine .....	25
Command Center .....	25
Connectors .....	31
Installation and Upgrade .....	31
Localization .....	34
Pattern Discovery .....	34

# ArcSight ESM 6.5c

---

These release notes discuss the following topics.

["Welcome to ESM 6.5c" on page 5](#)  
["What's New in This Release" on page 5](#)  
["Upgrade Support" on page 8](#)  
["Geographical Information Update" on page 9](#)  
["Vulnerability Updates" on page 9](#)  
["Supported Platforms" on page 9](#)  
["Verifying Secure Delivery" on page 9](#)  
["Usage Notes" on page 10](#)  
["Frequently Asked Questions about ESM with CORR-Engine" on page 11](#)  
["Fixed Issues in ESM 6.5c" on page 14](#)  
["Open Issues in ESM 6.5c" on page 17](#)

## Welcome to ESM 6.5c

ESM delivers ArcSight's world-class Security Information and Event Management (SIEM) with ArcSight's proprietary storage solution, the Correlation Optimized Retention and Retrieval (CORR)-Engine. The CORR-Engine powers ESM's superior correlation capabilities with significant performance improvements over the Oracle storage.

## What's New in This Release

This section describes the new features and enhancements added in this release.

### ArcSight Command Center

The ArcSight Command Center is a web-based user interface for ESM. It enables you to perform many of the functions found in the ArcSight Console and ArcSight Web, also provided with ESM. It provides you the ability to:

- View dashboards, do several kinds of searches, run reports, do case management, notifications, and administrative functions for managing content, users, connectors, storage, archives, search filters, saved searches, and peer configuration.
- Synchronize your ESM content across multiple instances from a primary ESM source, where all configurations are done, to multiple ESM destinations using the Content Management feature. Synchronization is supported for all packages except those including any of these resources: Actors, Assets or Asset Ranges, Cases, Connectors, Packages, Partitions, Active or Session Lists, or Database Table Schemas.
- Establish peer relationships with other ESM instances and perform searches across peers.

- Saved Searches and Search Filters appear on the ArcSight Console resource tree to leverage the resource grouping and packaging features.
- Add and configure up to four storage groups in addition to two the come out-of-box. Each storage group can have its own retention policy and archive settings. Send events from a specific connector to a specific storage group using storage mappings.
- Display context-sensitive online help.

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

## Rules

- Pre-persistence rule type  
A pre-persistence rule type is now available. This event-enriching rule calls the Set Event Field action to modify base events before they are persisted in storage, unlike other rule types that set fields on rule correlation events. Event fields are modified every time an incoming event matches the condition specified for the rule. The rule does not have to wait to go through the process flow before executing the action. Event fields set by a pre-persistence rule are available to normal, real-time rules that run during post-persistence flow.
- Rule actions to create and update a case  
The rule actions, Create a New Case and Add to Case, now provide the ability to set case attributes, such as ticket type, stage, frequency, and so on.

Refer to the topic "Rules Authoring" in the ArcSight Console User's Guide for more information about rules.

## Lists

- You can now specify active and session lists to be case-sensitive or case-insensitive. You can further refine the case insensitivity setting for key fields only, value fields only, or both.
- Active and session lists can now support up to 5 million entries. Details for the required setups are in the topic "List Authoring" in the ArcSight Console User's Guide.
- The IPv6 address format is now supported. This address is available as a subtype for the Address data type in active and session lists.

Refer to the topic "List Authoring" in the ArcSight Console User's Guide for more information about lists.

## Reports

If you are sending a PDF, XLS, RTF, or CSV-formatted report as an email attachment, you can choose to compress (zip) that report before sending it.

Refer to the topic "Building Reports" in the ArcSight Console User's Guide for information about reports.

## Cases

A case can now include correlated base events when you manually create a case or when a rule action creates or updates a case.

Refer to the topic "Rules Authoring" in the ArcSight Console User's Guide, for more information about rules. Refer to the topic "Case Management and Queries" in the ArcSight Console User's Guide for information about cases.

## Actors

ESM now supports up to 500K actors. The Actor Model Import Connector has been enhanced to support the new limit.

Refer to the topic "Actors" in the ArcSight Console User's Guide for more information about actors.

## Saved Searches and Search Filters

The ArcSight Console now includes two new resources on the resource navigator panel: Saved Searches and Search Filters. Configuration for these resources are done on the ArcSight Command Center. On the ArcSight Console, you can leverage the resource grouping and packaging features for these resources.

For details about creating searches and filters, refer to the following topics in the ArcSight Command Center User's Guide:

Searching for Events > Saved Queries (Search Filters and Saved Searches)

Administration > Search Filters

Administration > Saved Searches

Refer to the topics "Editing Resource Groups" and "Managing Resources" in the ArcSight Console User's Guide for details about resource groups and packages, respectively.

## Variable Functions

This release provides the following new and enhanced variable functions to support list authoring.

- **GetListElement** is a new function that returns the element at a specified index in a list of elements.
- **ConvertStringToIPAddress** is a new type conversion function that converts an IP address stored in string format into an IP address type.
- **ConvertStringToList** is an enhanced type conversion function that now provides an optional second parameter for you to set a separator string, such as a pipe (|), in addition to the default comma separator.
- **AliasField** is an enhanced Alias function that was previously available only to event schemas. Now, you can use this function in all schemas such as Actors, Cases, and so on.
- **Value List** is a new function category containing GetListElement (a new function) and GetSizeOfList (moved from Type Conversion).

Refer to the topic "Variable Functions" in the ArcSight Console User's Guide for information about variables and functions.

## Event Priority Rating

You can now view an event's priority rating, or score, through the Debug Event Priority option. When you right-click an event on a channel, a popup displays the priority score calculated for the selected event.

Refer to the topic "Priority Calculations and Ratings" in the ArcSight Console User's Guide, for more information about the Threat Level Formula that calculates priority scores.

## Migration of ESM Resources from Oracle to CORR-Engine

A utility is now available to help customers migrate their ESM resource data from Oracle to CORR-Engine without engaging HP ArcSight Professional Services.

Refer to the document, "Migrating ESM Resources from Oracle to CORR-Engine," for instructions.

## ArcSight Risk Insight

ArcSight Risk Insight is an add-on product that enables users to understand the business impact of real-time threats on assets. In ESM, users define asset business layers (including workstations, servers, laptops), use rules to calculate risks factors on these assets, and import the data into Risk Insight. Risk Insight aggregates the scores following the business model, and users assess the impact of a specific threat that could present a risk factor on the business. Users build their own key performance indicators to monitor their organization's business risks continuously. Once installed, Risk Insight is accessed through the ArcSight Command Center.

Refer to the Risk Insight User's Guide for details.

## Upgrade Support

Direct upgrade to ESM 6.5c is supported **only** from ESM 6.0c.

## Upgrade From ESM 6.0c

Refer to the ESM 6.5 Upgrade Guide for instructions on how to upgrade your ESM 6.0c installation to ESM 6.5c.

## Migrating from ESM 5.x to ESM 6.5c

This release of ESM does not support a direct upgrade path from your ESM 5.x installations to ESM 6.5c. However, if you would like to migrate from a version prior to ESM 6.0c (5.x), you must do the following in the order listed below:

- 1 Install ESM 6.0c on a machine other than your existing ESM 5.x installation machine. Refer to the ESM 6.0c Installation and Configuration Guide for detailed steps to do so.
- 2 Migrate the resources from your existing ESM (effectively from the underlying Oracle database) to the newly installed ESM 6.0c.

ESM 6.0c uses CORR-Engine as its backend. The CORR-Engine-based ESM requires a fresh installation. If you would like to migrate your resources from an existing (legacy) ESM installation, you should do so on a **freshly installed** ESM on which resources have not been altered or added. Any resources that are changed or added after the ESM 6.0c installation along with their associations with any events will be wiped out while migrating the resources. Use the Resource Migration tool to migrate your resources from Oracle to the CORR-Engine.

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

Contact your HP Account Representative, if you plan to migrate your resources from your legacy ESM installation, to discuss your specific requirements and coordinate migration during the installation of the ESM 6.0c software.



The Resource Migration tool is available for download from the HP Software Depot at <http://support.openview.hp.com/downloads.jsp>. Refer to the Migrating ESM Resources From Oracle to CORR-Engine document which can be downloaded from the HP SSO website, for detailed steps to do so.

- 3 Upgrade to ESM 6.5c. Refer to the ESM 6.5c 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\_2013901**.

## Vulnerability Updates

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

- Snort / Sourcefire SEU-957 updated Faultline, Bugtraq, CVE, Nessus
- Enterasys Dragon IDS updated CVE
- Cisco Secure IDS S741 updated Bugtraq, CVE
- Juniper / Netscreen IDP update 2298 updated Faultline, CVE, Nessus, MSSB
- TippingPoint UnityOne DV8469 updated Bugtraq, CVE
- ISS SiteProtector updated Faultline, Bugtraq, CVE, X-Force, Nessus, CERT
- Symantec Endpoint Protection updated Bugtraq, CVE
- McAfee HIPS 7.0 updated CVE
- Radware DefensePro updated CVE

## Supported Platforms

ESM 6.5c is supported on Red Hat Enterprise Linux 6.4 64-bit platform for fresh installation and Red Hat Enterprise Linux 6.2 64-bit for upgrades. Refer to the Product Lifecycle document available on the Protect 724 site for further information on supported platforms and browsers.

### ESM Patches

This release includes fixes released with ESM 6.0C Patch1 but fixes in ESM 6.0c Patch2 are not included in this release of ESM 6.5c.

## 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

### Forwarding Connector

Make note of the following for the Forwarding Connector for ESM 6.5c:

- The Forwarding Connector for ESM 6.5c is only supported on Red Hat Enterprise Linux 6.4 64-bit.
- ESM 6.5c supports upgrading to Forwarding Connector 6.0.4.6830.0 from the previous Forwarding Connector release 5.2.5.6403.0. If you are installing ESM 6.5c in a hierarchical environment, please install Forwarding Connector 6.0.4.6830.0 directly.
- If you are forwarding events from ESM 5.5 or ESM6.0c, the Forwarding Connector version used must be the one released with the latest ESM version, in this case version 6.0.4.6830.0.
- The automatic forwarding of base events offered with the Correlated Forwarding Connector feature is **not** supported for ESM 6.5c. On-demand pulling of events is supported.

### Domains

The Domains feature is not supported for this release.

### Browser Support in FIPS with Suite B Mode

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

You cannot use the Internet Explorer browser to connect to the Manager, since Internet Explorer does not support FIPS with Suite B.

### 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 6.5c are different than the commands for starting and stopping components that were used in prior releases of ESM with Oracle backend.

Also, in ESM 6.5c, 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 supported "arcsight\_services" enter the following command while logged in as user "arcsight":

```
/sbin/service 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.

## Discover Fields List - Top Values and Values by Time

The **Field Summary > Discover Fields** option in the Command Center Search feature is not supported in ESM 6.5. If you search a version 5.3 SP1 peer Logger using the ArcSight Command Center search feature, check both the Field Summary and Discover Fields options, run a search, the "Values by time" link in the pop-up for any field in the "Discovered Fields" list will not work.

**Workaround:** To use the Discover Fields option, run the search from the 5.3 SP1 Logger.

## Frequently Asked Questions about ESM with CORR-Engine

The following section answers some frequently asked questions about ESM with CORR-Engine.

### **How many machines do I need for installing ESM 6.5c? What platform is ESM 6.5c supported on?**

The ESM Manager and CORR-Engine components come integrated in a suite that is installed on a single machine. Single machine install provides better scalability with localized processing and storage tiers. ESM 6.5c should be installed on a single Red Hat Enterprise Linux 6.4 64-bit machine. The Manager and CORR-Engine cannot be installed on separate machines.

See the section, ["Supported Platforms" on page 9](#), for more information on supported platforms.

### **How do I plan my hardware requirements in order to get the maximum performance from CORR-Engine?**

The ESM 6.5c CORR-Engine solution scales better with additional cores. The more the CPUs used, the better the performance. When compared to Oracle, the CORR-Engine is less dependent on I/O. Call the HP Professional Services for help with the sizing requirements.

### **What are the hardware requirements for ESM 6.5c?**

Refer to the "System Requirements" section in the "Installing ESM" chapter of the ESM Installation and Configuration Guide.

### **Can ESM 6.5c be part of a mixed hierarchical architecture with ESM 5.x using a Forwarding Connector?**

Yes. You can forward events from ESM 5.0 SP2 with latest patch or 5.2 with latest patch to ESM 6.5c. However, we recommend that you do not send events to ESM 5.x, and instead send them directly to ESM 6.5c.

### **Will existing licenses work?**

If you have a valid existing ESM license, you can use it with ESM 6.5c.

**Can I continue to use my existing Loggers with ESM 6.5c?**

Yes. You can forward events from Logger 5.3 to ESM 6.5c and vice versa.

**Can I upgrade my existing ESM installation to ESM 6.5c?**

Direct upgrade is supported **only** from ESM 6.0c to ESM 6.5c.

Direct upgrade of an ESM 5.x installation to ESM 6.5c is **not** supported. Refer to the section, ["Migrating from ESM 5.x to ESM 6.5c" on page 8](#) for more details.

**How do I get to manage.jsp?**

`manage.jsp` and other advanced troubleshooting tools, such as `license.jsp` and `resource.jsp`, are available from the new ArcSight Command Center Console using this URL:

```
https://servername:8443/arcsight/web/manage.jsp
```

`manage.jsp` and the other advanced troubleshooting tools are not supported for general customer use without guidance from HP Customer Support.

**Does the CORR-Engine use event side tables?**

The CORR-Engine does not use event side tables. You see a significant improvement in the CORR-Engine's performance over Oracle because the need to join with side tables is eliminated in the CORR-Engine.

**Can I archive my events with CORR-Engine?**

Yes, the event archiving functionality in CORR-Engine works in a similar way as it did in ESM 5.x with Oracle. There is significant improvement in this feature, such as:

- better compression
- faster reactivation/deactivation
- easy to use
- no DBA needed
- has a web interface
- easier to scale

See the ESM Administrator's Guide and the ArcSight Command Center User's Guide for further details.

**How do I backup and restore my data in ESM 6.5c?**

Refer to the ESM Administrator's Guide and the ArcSight Command Center User's Guide for details on how to backup and restore your data.

**How/When do I migrate my resources from my legacy ESM installation?**

You will need to install ESM 6.0c first. Once you have installed the ESM 6.0c software, you can migrate your resources from a legacy ESM 5.x installation. See ["Upgrade Support" on page 8](#) for more details.

The resource migration tool migrates only the resources. It does not migrate event data or events attached to cases. Keep your existing ESM instance running to capture historical data according to your retention policies.

If you would like to migrate your resources from an existing (legacy) ESM installation, you should do so on a freshly installed ESM 6.0c on which resources have not been altered or added. Any resources that are changed or added after installation along with their associations with any events will be wiped out while migrating the resources.

**What fields are indexed in CORR-Engine?**

The CORR-Engine indexes every field, including customer-created fields. The CORR-Engine does not index LOB-based fields, whereas Oracle only had a subset of fields that were indexed. You do not need to add any custom indexes. This speeds up the searches significantly.

**Can the storage size of the CORR-Engine be changed after installing the product?**

Yes. Please contact HP Professional Services through your HP Account Representative for information and assistance on this.

**How do I view my archive/storage info?**

You can view your archive and storage information using the ArcSight Command Center.

**How does CORR-Engine do compression on archives?**

The CORR-Engine's archive file size is smaller than that of Oracle. You do not need to use GZIP on data files since data is compressed inside the data files.

**Are there any Oracle-based ESM features that are not supported in CORR-Engine-based ESM?**

- The Domain feature is not supported in CORR-Engine-based ESM.
- Auto-forwarding of base events is not supported.
- Daily partitioning on trend and session list data is replaced by weekly partition.

## Fixed Issues in ESM 6.5c

### Analytics

Issue	Description
NGS-6359	A trend would fail to run if the trend query contained a custom conditional evaluation.  This issue is fixed. The trend query can now contain a custom conditional evaluation.
NGS-5266	A query that is used in a report, query viewer, or channel that uses event annotation could affect the system performance if it has a large event annotation data. This is still an issue, but can be fixed by optimizing the query dynamically. To do so, set the event.annotation.optimization.enabled flag in the /opt/arc sight/manager/config/server.properties file to true.
NGS-3686	Users can now delete a Trend used in a Query that in turn is used in a Query Viewer.

### ArcSight Console

Issue	Description
ESM-50538	The Add, Remove, and Replace column selector has been reverted back to the same look as previous ESM versions, such that it moves the root level columns back into a "root" group.
ESM-47163	The previous releases were missing a variable function to convert a string to an IP address. A new variable function, ConvertStringToIPAddress, has been added in this release to convert a string to an IP address.
ESM-46773	In this release, there is an added option in the email format to compress a scheduled report before emailing. The option is, 'Attach Compressed Report,' under Report Parameters.  The new feature is documented in the What's New for ESM 6.5c, and in the ArcSight Console User's Guide, in the "Building Reports" topic under the subtopic "Report Parameters: Default and Custom."
ESM-33943	If you moved a resource, the search result would output the wrong URI even if you ran a Resource Search Index Updater. At the same time, the URI shown in Resource properties was correct and matched the updated location. This has now been fixed and the search result outputs the correct URI if you run a Resource Search Index Updater.
ESM-33489	When a connector was updated or the Manager restarted, occasionally it showed an incorrect user name in the editor. Now, when it is changed by a user, it shows the correct username. If the Manager is restarted, then it shows a blank username.
NGS-5582	There were performance issues in the ArcSight Console when navigating through the groups. The ArcSight Console was slow when Dashboards were open in a low-bandwidth/high-latency network.  This issue is now fixed and the ArcSight Console's performance is as expected.
NGS-4387	Previously the HTML text in a payload viewer used non-HTML line breaks. These are now replaced with HTML line breaks:  .

Issue	Description
NGS-3129	<p>When you selected the geographic view from events in an active channel, both Longitude and Latitude information were shown as 0.</p> <p>This bug is fixed and now the geographic view shows the correct Longitude and Latitude information for the events.</p>
NGS-1072	<p>Displaying EventGraph data monitors from within the ArcSight Console custom layout internal browser is no longer supported. You must launch an external browser from the ArcSight Console custom layout or use the ArcSight Command Center dashboard module in order to view any dashboard with EventGraph data monitors.</p>

## ArcSight Manager

Issue	Description
ESM-50704	<p>An export would fail to complete using the package command.</p> <p>This is now fixed. Now you can export large packages using the CLI command in standalone mode.</p>
NGS-5483	<p>Excessive temporary file space gets used when Group By (or sorting) is performed on the Event table. This issue now has a workaround.</p> <p>Workaround: Use the ArcSight substring function on varchar/string event fields to minimize the data manipulation during grouping. You can use existing local or global variables to achieve this behavior and replace the existing field in the query with the variable.</p> <p>If the file space usage is still not satisfactory, you can convert the character set automatically to Latin which uses less space. To do so, set the <code>event.query.charset.conversion</code> property to 1 in the <code>/opt/arc sight/manager/config/server.properties</code> file to convert the existing charset to latin1. Alternatively, set the property to 2 for conversion to binary and then to Latin (to minimize conversion error for non-English character set). The default value of this property is zero.</p> <p>Note: Use this property carefully to avoid character conversion error of multi-byte character to one byte (latin1) truncation.</p>
NGS-4335	<p>A memory leak in the CORR-Engine which caused the Manager to become unresponsive has been fixed in this release.</p>
NGS-4202	<p>Even though an initial query for event data timed out, the Active Channel would show the status as "Loading...". An issue that caused the Active Channel to stay in "Loading..." forever has now been fixed.</p>

## ArcSight Web

Issue	Description
ESM-50148	<p>An issue where session cookies for ArcSight Web were set on the client web browser without the HTTPOnly directive enabled has now been fixed.</p>
ESM-49935	<p>Previously, the exception stack would display in the page source. This is now fixed by the addition of a new property. To NOT display the exception stack in page source, add the following property in <code>webserver.properties</code>:</p> <pre>web.display.exception.stack=false</pre> <p>Then clear the browser cache.</p> <p>This is now documented in the "Preferences" section of the ArcSight Web User's Guide.</p>
NGS-4219	<p>A report would fail to run if a web user logged in to ArcSight Web and selected a user's email address using the 'Email to' button. The problem occurred when the web user was configured with an Active Directory external id.</p> <p>This issue is now fixed. You can now use the 'Email to' button to select a user's email address successfully.</p>
NGS-4056	<p>The payload value in ArcSight Web was HTML encoded and an XSS vulnerability was encountered. This issue is now fixed and you will no longer encounter an error.</p>



## CORR-Engine

Issue	Description
NGS-4229	Archive stopped working after the Daylight Saving Time ended in Brazil at midnight on 10/22 when the clock was turned back one hour. The following error appeared in the Logger log file: "An archive with duplicate date already exists in the database". This issue is now fixed and this error no longer appears in the log file.

## Open Issues in ESM 6.5c

### Analytics

Issue	Description
ESM-49283	<p>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:</p> <p><a href="https://&amp;lt;hostname&gt;;8443">https://&amp;lt;hostname&gt;;8443</a></p> <p>Such an event is retrieved correctly with the filter 'Request Url Host Is Not Null' (do not use filter 'Request Url Host != Null' as this is an invalid filter).</p>
ESM-48858	System audit events, such as those resulting from a rule being disabled by the system, are given a low TTL (time-to-live) value to prevent excessive rule triggering. A single rule can correlate such audit events, but any subsequent chaining rules are suppressed.
ESM-48307	If you have the Compliance Insight Package for IT Governance, note that the DeviceEventclassId for Windows 2008 has the same value as Windows 2003.
ESM-40449	When exporting events from the Case Details channel, archived events are not exported.
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-35070	<p>Verify Rules with Events (replay with rules) does not work for the following types of active lists if one of the rules adds to the active list and the second rule uses that data in a condition:</p> <ul style="list-style-type: none"> <li>- An event-based active list with values</li> <li>- A field-based active list with values, where all fields are mapped to event fields</li> </ul> <p>Verify Rules with Events does work for other types of active lists and when only one rule is used. Also, valid active lists work properly with real-time rules when they are deployed, including the two types of active lists described above.</p>
ESM-34531	When you set the Schedule Frequency for a report, the Next Run Time field is displayed incorrectly in the Editor. Even though the time is displayed incorrectly, the report runs at the time specified in the editor.

Issue	Description
ESM-29633	<p>Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (for example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.</p>
ESM-29348	<p>For trends, the Scheduled Time column in the Scheduled Runs view covers both time ranges for runs that have already occurred and for runs that are pending. As a result, you will see some discrepancy in the time ranges shown in the column. For example, against the runs that have already occurred, you will see the lower end of the time range. (For trends set to run hourly, if the time range is between 1:00 pm - 2:00 pm you will see 1:00 pm). The pending runs show the upper range (if the time range is between 1:00 pm - 2:00 pm you will see 2:00 pm). Trends that have already occurred will have a time difference that reflects the trend query schedule (for example, one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (for example, 24 hours if run once a day).</p>
NGS-7906	<p>In a Query, the GetHour variable returns the hour translated from local time to GMT. For example, if your local time is 20:31:47, the GetHour variable might return 3, instead of 20, as expected.</p>
NGS-7896	<p>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.</p>
NGS-7876	<p>If the ConvertStringToList variable function was used in any resources prior to upgrading to 6.5c, those resources will be broken after upgrade, and the variables (local or global) will display as empty definitions in the editor.</p> <p>Workaround: open the affected variable and reenter the function and parameters.</p>
NGS-7865	<p>A rule will be marked invalid if it contains a condition using the ContainsValue operator.</p> <p>Workaround: move the condition to a Filter, and use a MatchesFilter condition in the rule.</p>
NGS-7181	<p>Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.</p>
NGS-6521	<p>The Day function does not convert time-stamp data correctly. For the event count history, this issue causes the Event Count Last 7 Days query viewer to show the wrong data.</p>
NGS-6509	<p>If you have the IdentityView 2.5 solution and have 500 K actors, the actor channels are not being loaded. This happens intermittently.</p>
NGS-5756	<p>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.</p>
NGS-4187	<p>Trend tables that exceed 1 GB may cause a signal 11 error in the CORR-Engine.</p> <p>Workaround: Keep trend tables small (&lt; 1G). Trends running on ESM with Oracle were often created to provide improved report performance on a subset of columns. This is no longer needed with CORR-Engine.</p> <p>The best way to reduce an overgrown trend table is to edit the trend and reduce the "retention" period. For the change to take effect, rerun the trend. If the trend data is no longer needed, you can delete the trend and the space that was used by the trend gets freed up.</p>

---

Issue	Description
NGS-3139	<p>While trying to query on a case, specify the ID of the user instead of the name of the user.</p> <p>For instance:</p> <p>if owner=admin, this will not work</p> <p>if owner=1UOtZMTkBABCA0qd7zsU1IQ==, this will work</p>

---

## ArcSight Console

Issue	Description
ESM-51217	<p>ContainsValue is an operator on the Common Conditions Editor which is not currently documented. ContainsValue is used where the left-hand-side operand is a list of some data type, and the right-hand side operand is a single value (field or literal) of the same data type.</p> <p>For example, a variable "IPList" is a list of IP Addresses obtained from a multi-mapped active list, with values {192.0.2.0, 192.0.2.1, 192.0.2.2}. The ContainsValue operator can be used in following conditions:</p> <p>IPList ContainsValue TargetAddress (This returns true or false depending on whether TargetAddress value is contained in IPList.)</p> <p>IPList ContainsValue 192.0.2.0 (This returns true because the right-hand side value is contained in IPList.)</p> <p>IPList ContainsValue 192.0.2.24 (This returns false because the right-hand side value is not contained in IPList.)</p> <p>ContainsValue can be used in both query and in-memory resources.</p>
ESM-51149	<p>The geographical location mapping for some IP addresses may be wrong. For example, the values in the source and target "Country Code", "Region Code", "Country Flag URL" and "Country Name" fields may be wrong.</p> <p>Workaround: None at this time.</p>
ESM-50470	The filter (Source FQDN Is NOT "") does not work on Active Channels.
ESM-49990	To display the correct icon for forwarded correlation events, add the Locality Field column to the field set of the channel.
ESM-47213	<p>Case-related events are copied to a special table so they can remain available after being archived. The channel is unable to find and display such events correctly after the partition is archived.</p> <p>Workaround: Use the case event editor or Reports, which can correctly find and display these events.</p>
ESM-41641	<p>On Mac OS X only: If you open a channel, select some rows, right-click on them and select Print Selected Rows from the resulting menu without a default printer set up, the Console will abruptly terminate.</p> <p>Workaround: Before you start the Console, make sure to set up a default printer to which to print.</p>
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	The Console can become unresponsive if you access other resources while building category models with a large number of actors.

Issue	Description
ESM-39829	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.
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 "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).</p>
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, no error will be displayed indicating that you are not able to view some resources in the query due to lack of sufficient permissions.
ESM-33462	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.
ESM-33440	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-26488	<p>If you import the content of an older package into an existing newer package, the contents from the two packages are merged. The resulting package will consist of contents from both packages. The relationships will be merged, but the attributes will be picked up from the old package.</p> <p>Workaround: Export the new package to a bundle file so that you can recover it if need be. Then delete the new package before you import the old one.</p>
NGS-7884	Four other packages are dependent on the ArcSight Core Security package, it is strongly recommended not to uninstall this package. However, notification actions should not be enabled in any rules under /All Rules/ArcSight Core Security if you really need to uninstall this package.
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.
NGS-7526	Non-admin users need to have read permission manually added to /All Trends/ArcSight Core Security for Default User group.
NGS-7233	<p>When using the ContainsValue operator in the Common Conditions Editor, the user is allowed to enter a value in the editor. However, this value is invalidated and an error message instructs the user to use the popup editor instead to input values. This happens for correct as well as incorrect values entered.</p> <p>The workaround is to use the popup editor instead of entering the values in the editor directly.</p>

Issue	Description
NGS-7173	The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.
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-4091	If the arc_notification_history and arc_notification_registry are too big, the ArcSight Console will hang.
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-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-1262	If a dashboard contains a Query Viewer that has a large row limit, the Console may hang while loading this dashboard in Custom Layout view. It is a good practice to keep the row limit of Query Viewers to less than 100 before viewing the dashboard in custom layout format.
NGS-1088	If a regular or inline filter with a condition involving Event Annotation Flag is applied to an Active Channel, the Active Channel will not load any events.  Workaround: Avoid using Event Annotation Flag in filter conditions.
NGS-146	In some cases, event-based Active Channels that include InCase filtering condition will not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit.

## ArcSight Manager

Issue	Description
ESM-47625	When exporting a case, the Creation Time is changed to the time of the export.
ESM-41331	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: To produce a correct report, run the resource validation script manually as follows:</p> <ol style="list-style-type: none"> <li>1. Run the script using "arcsight resvalidate."</li> <li>2. Run the script again using "arcsight resvalidate -persist false."</li> </ol> <p>In general, the resource validation script should be run twice: the first time with '-persist true' (the default) to validate and fix invalid resources, and the second time with '-persist false' to generate a correct report.</p>
ESM-40889	The "group:101" audit event might not be sent when there are many role memberships being added or changed for an actor. An error about this is written to the server log, indicating the IDs of the affected objects.
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-31433	<p>The following exception might appear in the Manager's log file:</p> <pre>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</pre> <p>Workaround: This error is not serious. It is automatically resolved within one week of the Manager startup during which time the Manager rebuilds the resource search index (done weekly). You may choose to ignore the error, or manually do a rebuild at any time by running the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create -m &lt;manager-hostname&gt; -u &lt;admin-user-name&gt; -p &lt;password&gt;</pre>
ESM-30670	<p>If the search index file becomes corrupted, the search index will be out-of-date and the following message appears in the Manager's log file:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Re-generate the index by issuing the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create -m &lt;manager-hostname&gt; -u &lt;admin-user-name&gt; -p &lt;password&gt;</pre>
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-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>Workaround: Avoid executing concurrent package operations. Schedule Content Management package pushes at a time when no one is installing or uninstalling packages.</p>

Issue	Description
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	<p>If the field size of an event exceeds 32 KB, that event does not get persisted.</p>
NGS-3803	<p>The command "arcsight manager-reload-config" fails to dynamically reload the configuration.</p> <p>Workaround: Restart the Manager after you make any configuration changes, such as those in the config/server.properties file.</p>
NGS-3294	<p>At very high EPS rates and with too many annotated events, the source Manager cannot send base events to the destination Manager.</p>
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	<p>Shutting down services by using the arcsight_services command might results 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.</p>
NGS-172	<p>Base events are not automatically annotated after rules trigger.</p> <p>Workaround: Set logger.base-event-annotation.enabled=true in server.properties and annotate the events manually.</p>



## CORR-Engine

Issue	Description
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"> <li>1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend.</li> <li>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.</li> <li>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.</li> </ol>

## Command Center

Issue	Description
LOG-12033	<p>Pipeline searches for IP address fields do not display the results correctly.</p> <p>Workaround: When running pipeline searches for IP addresses, use field's Display Name; do not use the CEF name.</p> <p>If the IP Address is not correctly displayed in the search results, you can click the + next to the event in the search results, and view the field in the RAW data.</p> <p>For the chart operator, do not use functions like avg(), min(), max() etc.</p> <p>Do not use the operators eval, replace, rex, and regex on IP address fields.</p>
LOG-12032	<p>Command Center search will return the error message "There is a problem: null" when charting the aggregation results certain fields, if you fail surround the field name with parenthesis, as in the following example.</p> <pre>...   chart sum bytesIn by deviceEventClassId span=5m</pre> <p>Workaround: If you receive this error message, check your query, and add parenthesis if needed, as in the following example.</p> <pre>...   chart sum(bytesIn) by deviceEventClassId span=5m</pre>
LOG-12018	<p>IPv6 addresses do not display properly in the results of Command Center Searches using the Chart operator.</p> <p>Workaround: You can view the values of the IPv6 fields in the list of Events in the regular search results.</p>
LOG-12017	<p>When you click an IPv6 address field name in Field Summary Selected Fields list, the Field Value is not properly displayed in the resulting dialog box.</p> <p>Workaround: You can view the values of the IPv6 fields in the list of Events in the regular search results.</p>
LOG-12016	<p>Command Center searches using the "where" condition with the field operators "&gt;=", "=", or "&lt;=" to search IPv6 fields do not return the correct results.</p> <p>Workaround: Rewrite your search to avoid using the "where" condition.</p>
LOG-8484	<p>The stdev function in the chart operator does not work on fields that have more than 10 digits. The result of such computations is a blank field.</p> <p>Workaround: None at this time.</p>

Issue	Description
NGS-7912	In peer search, the search result is not refreshed responsively if one peer node has high hits or it's busy due to high injection rate or multiple searches running. As a workaround, cancel the search and ensure that the peer node has enough resources to process the search.
NGS-7907	When user perform peer search using IN operators for IP, MAC 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-7888	The fields listed in the Export Options dialog box may vary based on the browser you are using and the user you log in with. Even though only a partial list of fields is displayed, all fields are exported when you have the All Fields checkbox checked.  Workaround: To export only certain fields, uncheck All Fields and enter the fields you want to include.
NGS-7861	When using Internet Explorer 10, nodes in the Event Graph Data Monitor are not displayed properly when viewed in ACC-Dashboards.  Workaround: Use Firefox or Chrome to view Event Graph Data Monitor properly.
NGS-7847	If you are a non-admin user, you cannot select yourself from the Resource selector in the Case Editor or if you select "Run as user" or "Email to" in the Report parameters dialog.  Workaround: The admin give this User's Group read permission. To do this, edit the Access Control List (ACL) for the group that the user belongs to, open the Resources tab, select "User" from the "Set Permissions for" drop-down, and add the Read permission.  Navigate to an existing user group and click Edit. The Editing User Group screen displays information about the group. Click Advanced Permissions. The Advanced Permissions screen displays the current permissions for that group. Open the Operations tab and click Add. The Permission Selector displays a list of available permissions. Select ArcSight System > Search Filter Operations. The parent permission, Search Filter Operations, makes its children, Search Filter Read, Search Filter Write, effective.  Workaround: is to give Read access to non-admin user group which user belongs to.

Issue	Description
NGS-7833	The default field set that is displayed in search results is a limited set. If you use any search pipeline operators that result in selecting specific fields (apart from the default set) or creating new ones, then these selected fields won't be displayed (nor highlighted) in the search results unless you select the "All Fields" field set.
NGS-7796	<p>While using the Command Center and switching between the Dashboards and Search sections, you may encounter a "Session Timeout" message that prompts you to log in again. If you log in again, the message and prompt are displayed in a loop.</p> <p>Workaround: If you see this problem, clear/delete all the cookies for this web site in your browser, and log in to the Command Center again. If your browser can be configured to never cache cookies, you may want to enable this setting.</p>
LOG-7651	<p>On the Internet Explorer browser, data is truncated in the Advanced Search calendar popup window. This issue affects users' ability to select a date using the date picker (icon) when setting CCE rules in the Advanced Search feature. When a user clicks the date picker, the calendar widget that comes up is not wide enough to display the full calendar content, truncating columns with the latter days of the week.</p> <p>Workaround: Use the Tab key to scan along the part of the calendar that is initially hidden, then use Shift+Tab to scan back in the other direction. Alternatively, use another browser, such as Firefox.</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-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.
NGS-7570	<p>When running very large report, the Report view becomes very slow and is unresponsive as report is being downloaded for viewing.</p> <p>Workaround: Run a very large report from 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	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	<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>

Issue	Description
LOG-7099	<p>When values for user fields such as sourceUserId, sourceUserName, destinationUserId, and cs1 contain "\n" character, the search results are not displayed correctly.</p> <p>Understanding: The current software interprets a value that contains "\n" as a newline character. For example, user name "nancy" in example domain, "example\nancy", is interpreted as "example[newline]ancy".</p> <p>Workaround: Disable the multi-line feature by adding the following properties to /user/logger/logger.properties. The following examples use the default values.</p> <ul style="list-style-type: none"> <li>- To on/off the multiline support search.multiline.fields.supported=true</li> <li>- To on/off the \\n and \\t support search.double.backslash.newlines.supported=false</li> <li>- To on/off the DOS/Windows path support for CEF and/or syslog search.keep.windows.path.cef=true search.keep.windows.path.syslog=true</li> </ul>
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>
LOG-7046	<p>The time displayed on the histogram might not match the event time. This behavior is observed when the /etc/localtime file is not symbolically linked to the correct timezone.</p> <p>Workaround: Make sure that the /etc/localtime file is symbolically linked to the correct timezone in the /usr/share/zoneinfo file as shown in the following example. Then, restart the system.</p> <pre>sudo ln -s /usr/share/zoneinfo/&lt;timezone&gt; /etc/localtime</pre>
LOG-6965	<p>When the time change due to Daylight Savings Time (DST) takes place, the following issues are observed on Logger:</p> <ul style="list-style-type: none"> <li>- The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram.</li> <li>- The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period.</li> <li>- The events received during 1 a.m. to 2 a.m. DST are displayed under the 1 a.m. to 2 a.m. standard time bucket, thus doubling the number of events in the histogram bucket that follows an empty bucket.</li> <li>- Because the 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram, the bucket labels might seem out of order. That is, 1:59:00 a.m. in DST may be followed by 1:00:00 in standard time on the histogram.</li> <li>- If the end time for a search falls between 1 a.m. and 2 a.m., all of the stored events might not be returned in the search results.</li> </ul> <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p>
NGS-6933	<p>The home page does not display the correct data monitors.</p> <p>Workaround: Manually add read permission to the Default User Group for the following data monitor:</p> <pre>/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/Current Connector Status</pre>

Issue	Description
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 &gt; 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	<p>Storage Group names are limited to contain only ASCII letters, digits and spaces.</p>
NGS-6026	<p>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.</p> <p>Workaround: Use Internet Explorer or Firefox browsers to avoid this issue.</p>
NGS-5888	<p>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.</p>
LOG-5181	<p>Search results are not highlighted for values that match the IN operator in a query.</p> <p>Workaround: None at this time. Highlighting works if there's only 1 item in the square brackets. As soon as there's more than 1, no highlighting occurs.</p>
NGS-3892	<p>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.</p>
NGS-2849	<p>If the refresh rate is set to a low interval so that the refresh happens too frequently, under slow network connections or when having network problems, this might impact browser performance and dashboard behavior.</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-1582	<p>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.</p> <p>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.</p>
NGS-1451	<p>If a custom view dashboard contains a query viewer with a large row limit, the browser may hang while loading this dashboard.</p> <p>Workaround: Set the row limit of Query Viewers below 100 before viewing the dashboard in custom layout format.</p>
NGS-1283	<p>Non-admin users cannot access the Users, Connectors, &amp; Configuration page in ArcSight Command Center, even when provided with the permissions to do so.</p> <p>Workaround: You must have administrator privileges to access the Users, Connectors, &amp; Configuration page in ArcSight Command Center.</p>

## Connectors

Issue	Description
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-3806	<p>Auto-import of the Manager's certificate does not work if your connector is installed in FIPS Suite B mode.</p> <p>Workaround: Import the Manager's certificate manually. Refer to the Configuration Guide for instructions on manually importing the Manager's certificate into the connector.</p>
NGS-3498	<p>The certificate auto-import feature in connectors will only import certificates from the initial configuration.</p> <p>Workaround: Any changes or additions to the destinations require you to manually import the certificate for those destinations.</p>
NGS-2052	<p>When using Asset Model Import Connector to import assets, the connector does not uniquely identify assets by Zone and a unique IP address or a unique host name.</p> <p>For updating existing assets, please make use of one of the following attributes to identify them:</p> <ul style="list-style-type: none"> <li>- An External ID, or</li> <li>- a resource ID, or</li> <li>- a URI</li> </ul>
NGS-1423	<p>On a Windows machine, upgrading a connector from the ArcSight Console will fail if any process is using the connector's "current" folder.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Make sure there are no files in the connector's "current" folder open.</li> <li>2. Start the connector by using Start &gt; Programs &gt; Connector Programs. Do not start the connectors using the "arcsight agents" command.</li> </ol>

## Installation and Upgrade

Issue	Description
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&amp;#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-7027	There might be some inconsistencies between a fresh install and an upgrade, such as rules that are disabled or missing.

Issue	Description
NGS-6996	There might be some data monitors disabled after the upgrade, while they are enabled in a fresh installation and vice versa.
NGS-6983	There might be some unassigned assets removed after the 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>
NGS-4874	During the resource upgrade or migration from 5.0 SP2 Patch 4 to AE 4.0 some exceptions related to the references to deprecated resources show up in the logs even though the resources are all valid.
NGS-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> <p>"java.lang.NoClassDefFoundError: Could not initialize class sun.awt.X11GraphicsEnvironment".</p> <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-3909	If you have a high-end system, as described in the System Requirements section of the ESM Installation and Configuration Guide, running content that requires a high level of system resources and/or high EPS, contact HP ArcSight Customer Support for instructions on how increase the heap size beyond 16 GB.
NGS-3871	Under certain circumstances, the Uninstaller may not be able to remove all ESM 6.0c files under the /opt/arcsight/ directory. Refer to the Troubleshooting appendix in the ESM Installation and Configuration Guide on how to do the cleanup manually.
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	<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"> <li>1. Do not reboot without running the setup_serivces.sh command while logged in as the "root" user.</li> <li>2. If you reboot without running the setup_services.sh command, uninstall and then re-install the product.</li> </ol>
NGS-3808	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.



Issue	Description
NGS-3445	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.
NGS-3344	This release supports ESM installation while logged in as user "arcsight" only.
NGS-3322	<p>Due to the timing of some components' start-up, there may be some harmless error messages in the log files such as:</p> <p>[FATAL][default.com.arcsight.logger.distributed.DirectConnection\$ReadChannel][run]</p> <p>java.io.IOException: end of communication channel</p> <p>[FATAL][default.com.arcsight.logger.distributed.ClientDirectConnection][run]</p> <p>java.nio.channels.ClosedChannelException</p>

## 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"><li>1. Log in to ArcSight Console and open the report.</li><li>2. Create the report with a Chinese name.</li><li>3. Select the report template.</li><li>4. Edit the template with "Open in Designer."</li><li>5. Edit the header and other fields which need to display in Chinese characters.</li><li>6. Set the fonts to Arial Unicode for the fields that need to display Chinese characters.</li><li>7. Save the template.</li><li>8. Run the report with PDF format.</li><li>9. Open the generated report with Acrobat Reader version 9 to check if the Chinese characters display properly.</li></ol>
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>

## Pattern Discovery

Issue	Description
ESM-35048	<p>A java.lang.InterruptedException might be logged in the Manager's server.std.out.logs file when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.</p>
NGS-3527	<p>Pattern Discovery jobs can be resource intensive. Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. HP recommends that you reduce the number of events over which the Pattern Discovery search runs and/or the frequency of Pattern Discovery jobs.</p>