

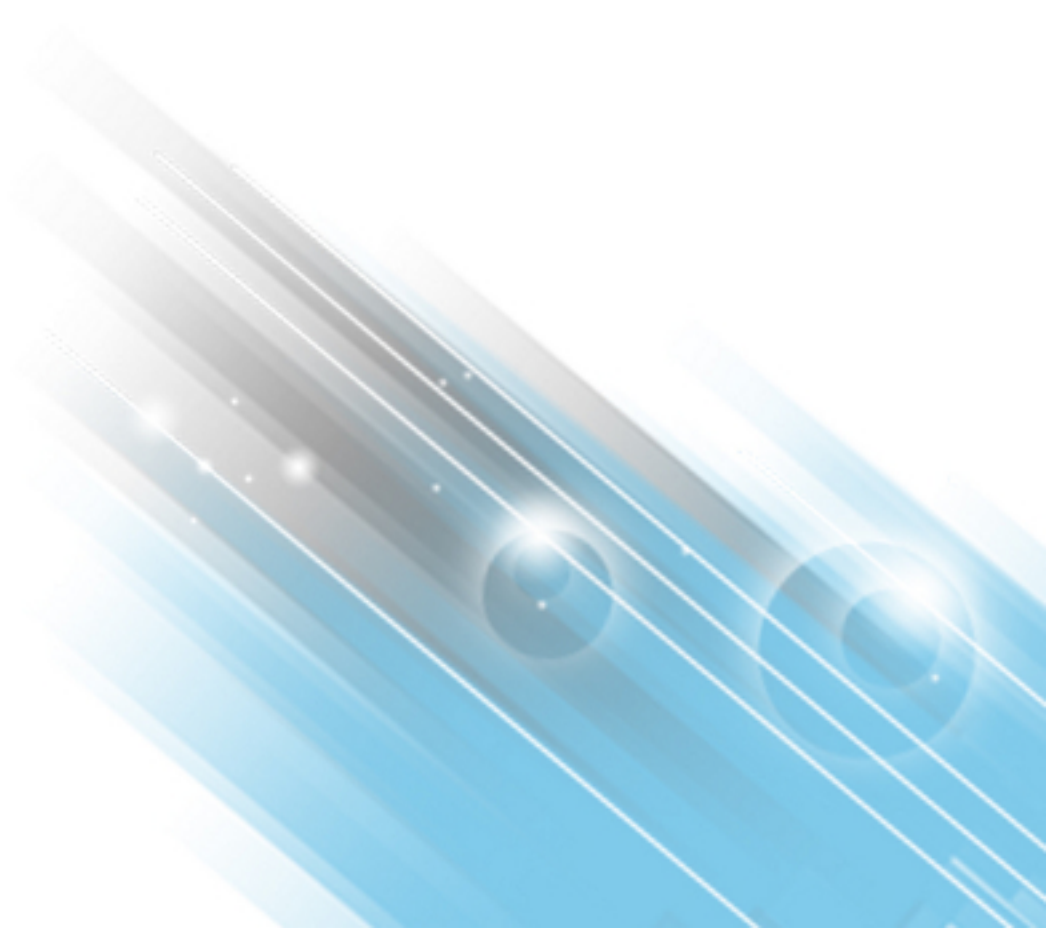


# HP ArcSight ESM

Software Version: 6.9.1c

## Release Notes

May 17, 2016



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2016 Hewlett-Packard Development Company, L.P.

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

<https://www.protect724.hpe.com/docs/DOC-13026>

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support Page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hp.com">https://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>

# Contents

ArcSight ESM 6.9.1c .....	5
Welcome to ESM 6.9.1c .....	5
What's New in This Release .....	5
Beta Feature: Superindexes .....	8
Verifying the Downloaded Installation Software .....	9
Upgrade Support .....	9
SuSE Linux No Longer Supported .....	9
Geographical Information Update .....	9
Vulnerability Updates .....	9
Supported Versions for Distributed Searches .....	10
Supported Platforms .....	11
Supported Languages .....	11
Usage Notes .....	11
Asset Model Import FlexConnector .....	11
Forwarding Connector .....	11
ArcSight Command Center Replaces ArcSight Web .....	12
Scroll Bar Issues with Google Chrome and Apple Safari .....	12
Localization .....	12
Configuring ArcSight Security Use Cases with the Use Case Wizard .....	12
ESM Unsupported Features .....	12
Menu Items Inaccessible in ACC Resized Window .....	12
Domains .....	12
Open Channels in the ArcSight Command Center .....	13
ESM Peer Certification for Content and Searches .....	13
Rearrange ACC Dashboard if Charts and Tables Overlap .....	13
Rules Recovery Timeout Possible .....	13
Push Status is Blank if a Subscriber is Offline .....	13
Identity View Not Supported .....	13
Disabling Full-Text Search to Save Disk Space .....	14
Open Issues .....	14
Analytics .....	14
Analyze/Search .....	15
ArcSight Console .....	15
ArcSight Manager .....	18
CORR-Engine .....	20

- Command Center ..... 21
- Connectors ..... 24
- Installation and Upgrade ..... 24
- Localization ..... 26
- SmartConnectors ..... 27
- Fixed Issues ..... 27
  - Analytics ..... 27
  - ArcSight Console ..... 28
  - ArcSight Manager ..... 29
  - CORR-Engine ..... 30
  - Command Center ..... 30
  - Configuration ..... 31
  - Installation and Upgrade ..... 32
- Send Documentation Feedback ..... 33

# ArcSight ESM 6.9.1c

## Welcome to ESM 6.9.1c

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

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

## What's New in This Release

This topic describes the new features and enhancements added in ESM 6.9.1c.



### **ArcSight Command Center**

#### **Enhanced Usage Reporting**

Usage Metrics: ESM usage reporting is available. This reporting feature displays daily EPS and GB for the last 30 days as both a chart and a grid. The report also displays the number of license overages in the past 30 days and the usage limit defined in the ESM license.

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






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





#### **Active Channel Improvements**

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

- Create, edit, and delete Event Channels.
- Modify field columns in the Channel Grid by adding and removing attributes.
- Apply Filter Conditions to Event Channels.
- Create an Event Channel by copying an existing Channel.

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

	<p><b>ArcSight Console Enhancements</b></p> <p>While editing a field set, you can now select multiple fields and move their position within the set.</p> <p>Refer to the topic, "Field Sets" in the ArcSight Console User's Guide.</p> <p><b>Enhanced Active List option on active channel</b></p> <p>You can now add your favorite active lists to the right-click Active List option on the active channel, saving you the extra steps of drilling down through the resource tree selector to select your list from various list groups. Create your favorite active list collection using the Console's Preferences menu.</p> <p>Refer to the topic, "Customizing the Selections for Active Lists" in the <i>ArcSight Console User's Guide</i>.</p>
	<p><b>Correlation Enhancement: Rule Resilience</b></p> <p>In this release, a resource-intensive deployed rule that causes EPS rates to drop is automatically disabled. The threshold for disabling is 50% of aggregate evaluation time of deployed rules.</p>
	<p><b>New Type Conversion Functions</b></p> <p>The following Type Conversion functions are introduced in this release:</p> <ul style="list-style-type: none"> <li>• ConvertStringToResourceReference</li> <li>• ConvertStringToIPv6Address</li> <li>• ConvertStringToMACAddress</li> <li>• ConvertStringToDate</li> </ul> <p>Use these functions to convert data types in your rules. Refer to the descriptions for Type Conversion functions in the topic, "Variable Functions," in the ArcSight Console User's Guide.</p>
  	<p><b>List Enhancements</b></p> <p><b>Active Lists</b></p> <p>You can now include the <i>Count</i>, <i>Creation Time</i>, and <i>Last Modified Time</i> fields in your active lists.</p> <p><b>Session Lists</b></p> <p>A new session list attribute, <i>TTL Days</i>, enables you to set the number of days a closed session should remain on the list, after which the session is removed.</p> <p>Refer to the topic, "List Authoring," in the ArcSight Console User's Guide.</p>

	<p><b>Security Use Cases</b></p> <p>Security Use Case packages are now available for download at <a href="https://saas.hpe.com/marketplace/arc-sight">https://saas.hpe.com/marketplace/arc-sight</a>. These packages provide essential security monitoring for network systems, and packages that monitor and analyze the event stream for critical security concerns.</p> <p>The security use case documentation is available on Protect 724 (<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>).</p>
	<p><b>Package Imports</b></p> <p>A property is introduced in this release:</p> <pre>esm.manager.disable.resource.move</pre> <p>The property is set to <code>true</code> by default. This disables moving existing resources to their new nodes and results in the resource being present in both hierarchies.</p> <p>Setting this to <code>false</code> in the <code>server.properties</code> file alters the hierarchy of resource nodes to conform with the new hierarchy.</p> <p>You can leave this setting to <code>true</code> under high loads to help prevent import failure for large packages, such as during zone update. Refer to the <code>zoneUpdate</code> command and “Editing Properties Files,” for details on editing the <code>server.properties</code> file, in the <i>ESM Administrator’s Guide</i>.</p> <p>Refer to the <i>ArcSight Console User’s Guide</i>, “Managing Packages” for information on packages in general.</p>
	<p><b>ESM Service Layer API</b></p> <p>A new method, <code>setAnnotationStage</code>, was added to the <code>SecurityEventService</code> service. This method provides the ability to set (annotate) an event’s stage, for example, from <b>Queued</b> to <b>Closed</b>. The new stage must comply with the stage transition workflow and other requirements. For example, the Follow-Up stage requires the user ID of the analyst responsible for acting on the case.</p> <p>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 with the ESM installation as HTML and as PDFs.</p> <p>For information about the Stages resource, refer to the topic, “Creating or Editing Stages” in the <i>ArcSight Console User’s Guide</i>.</p>
	<p><b>ESM Event Data Transfer Tool</b></p> <p>The Event Data Transfer Tool enables you to export ESM events into the Hadoop Distributed File System (HDFS) version 2.5.2 from Apache.</p> <p>Refer to the document, <i>ArcSight Event Data Transfer Tool User’s Guide</i>, for feature descriptions and procedures to install, configure, and use the tool.</p>



### zoneUpdate Administrative Command

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

`zoneUpdate` performs these actions in the Global network:

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

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

The zoneUpdates Subscription Package is available for download at <https://saas.hpe.com/marketplace/arcsight>.

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



### Authentication

#### FIPS Support

The recommendations for creating ESM's key pairs in FIPS Suite-B mode were changed to reflect IE, Chrome limitations and still be compliant with FIPS requirements. Cipher suite support has been reduced to the more secure options. In FIPS mode the default protocols include TLSv1.0 and 1.1. FIPS-related topics have been updated. Refer to "Appendix E: Configuration Changes Related to FIPS" in the ESM Administrator's Guide.

#### PKCS#11 Support

ESM now has extended PKCS#11 support to include a wider variety of vendors and configurations.

## Beta Feature: Superindexes

Superindexes are a feature available to qualified customers on a test basis in ESM 6.9.1c. 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 HPE Solution Architect to contact Product Management to determine eligibility to participate in the Beta and activate this feature.

## Verifying the Downloaded Installation Software

HP provides a digital public key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

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

## Upgrade Support

Direct upgrade to ESM 6.9.1c is supported from 6.5c SP1 with the latest patches or ESM 6.8c, with the latest patches. However ESM 6.8c does not support FIPS.

Note that HP does not support upgrades for AE 4.0 Patch 1 on G7 hardware. AE 4.0 Patch 1 upgrade is only supported on G8 hardware. If AE installation has an ArcSight Express security update applied, the ESM upgrade to 6.9.1c cannot proceed with the update in place. Follow the instructions in the documentation that accompanies the ArcSight Express security update to remove the update before proceeding with the ESM 6.9.1c upgrade.

## SuSE Linux No Longer Supported

SuSE Linux is no longer a supported operating system platform for ESM. Therefore, upgrades from ESM 6.5c SP1 or 6.8c on SuSE to ESM 6.9.1c are not supported. HP recommends upgrading to the latest patches.

For details on supported platforms, refer to the HPE ArcSight ESM Support Matrix available on Protect 724 (<https://www.protect724.hpe.com>).

## Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeolP-532\_20151101.

## Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU 1377 updated	Faultline, Bugtraq, CVE, Nessus
Cisco Secure IDS S894 updated	Bugtraq, CVE
Juniper / Netscreen IDP update 11-10-15 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, CERT
McAfee Intrushield updated	Faultline, CVE, Nessus, MSSB
IBM Enterprise Scanner 1.139 updated	CVE, X-Force
IBM Security Host Protection for Desktops 3190 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 35.110 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3190 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 35.110 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 35.110 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Server IPS for Linux technology 35.110 updated	Faultline, CVE, Nessus, X-Force
IBM RealSecure Server Sensor XPU 35.110 updated	Faultline, CVE, Nessus, X-Force
McAfee HIPS 7.0/8.0 content version 6753 updated	CVE

## Supported Versions for Distributed Searches

Distributed searches are supported from ESM 6.9.1c to the following versions of ESM and Logger peers:

- ESM 6.9.1c
- ESM 6.8c
- ESM 6.5c SP1
- Logger 6.1
- Logger 6.0

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 Platforms

See the ESM Support Matrix document available on Protect 724 (<https://www.protect724.hpe.com>) for details on ESM 6.9.1c platform and browser support.

## Supported Languages

These languages are supported by ESM:

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

## Usage Notes

### Asset Model Import FlexConnector

The Asset Model Import FlexConnector supports the ability to create and manage the Asset Model within ESM. The Asset Model Import FlexConnector allows you to develop a model import connector to import asset model data from a file. This enables you to create and maintain ESM Network Model data and keep the data in sync with the data in your Asset Management system. The Asset Model Import FlexConnector to install for ESM 6.9.1c is version 7.1.7.7604.0. See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.9.1c supported platforms.

### Forwarding Connector

The Forwarding Connector can receive events from a source Manager and then send them to a secondary destination Manager or to an ArcSight Logger. The Forwarding Connector to install for ESM 6.9.1c is version 7.1.7.7602.0. Only the Linux executable applies to ESM 6.9.1c. See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.9.1c supported platforms.

## ArcSight Command Center Replaces ArcSight Web

ArcSight Web is replaced by the ArcSight Command Center (ACC) . The ACC provides dashboards, several kinds of searches, reports, case management, notifications, and administrative functions for managing content, users, connectors, storage, archives, search filters, saved searches, and peer configuration. See the HP ArcSight ESM Command Center User's Guide for details.

## 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.

## 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.

## Configuring ArcSight Security Use Cases with the Use Case Wizard

Some ArcSight security use cases require additional configuration using the Use Case Configuration Wizard. These use cases include Reconnaissance, Anomalous Traffic Detection, Brute Force Attack, Firewall Monitoring, Suspicious Outbound Traffic Monitoring, and VPN Monitoring. If you have more than 150k assets, the configuration may take several minutes, during which the ArcSight Console may appear unresponsive. This is expected behavior; the configuration will succeed eventually.

ArcSight Security Use Cases are available for download from <https://saas.hpe.com/marketplace/arcSight>.

## ESM Unsupported Features

See the ESM Support Matrix document available on the Protect 724 (<https://www.protect724.hpe.com>) site for details on ESM6.9.1c unsupported features.

## Menu Items Inaccessible in ACC Resized Window

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

## Domains

The Domains feature is not supported for this release.

## Open Channels in the ArcSight Command Center

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

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

## ESM Peer Certification for Content and Searches

Peering is automatically mutual, so a group of peers may be enabled from a single Manager. Content Management is certified with up to five subscribers, with one additional Manager as a publisher. Peer searches are also certified with 5 peers

## Rearrange ACC Dashboard if Charts and Tables Overlap

In ACC, if the default dashboard displays charts and tables that overlap, use **Edit > Auto Arrange** or **Edit > Arrange** to reorganize the charts and tables in the dashboard. Click **Save** to save the new dashboard layout. See the topic "Change the Location of a Dashlet" in the ESM Command Center User's Guide for more details on arranging dashboards.

## Rules Recovery Timeout Possible

Rules recovery can timeout if there is a high EPS on the system, which causes the server to stop loading events from the database for checkpoint. You can modify the `rules.recovery.time-limit` property in `server.properties` to set a higher recovery time limit to attempt to prevent this timeout. The default value for the `rules.recovery.time-limit` property is 120 seconds (two minutes).

**Note:** The timeout can still occur even after you increase the time limit, due to overall system load, high EPS, or a large number of rules to recover.

For details on editing the `server.properties` file, see the "Editing Properties Files" topic in the ESM Administrator's Guide.

## Push Status is Blank if a Subscriber is Offline

The Push Status field in Push History shows a value only for subscribers that are online. If a peer is not online, the Push Status field in the Push History is blank.

## Identity View Not Supported

ESM 6.9.1c does not support IdentityView.

## Disabling Full-Text Search to Save Disk Space

Full text search (the ability to search on any word of any text field of an event) is enabled by default. However, full text search takes more disk space than if it is disabled. With it disabled, the disk space needed for storing events is only about 65-70 percent of what is required with full text search enabled.

To disable it, add the following line to the `server.properties` file and restart the ESM manager:

```
fulltext.search.enabled=false
```

## Open Issues

This release contains the following open issues.

## Analytics

Issue	Description
ESM-49283	<p>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:</p> <pre>https://hostname.example.com:8443</pre> <p>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 <code>!=</code> makes the filter invalid.</p>
ESM-39405	<p>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.</p>
NGS-17561	<p>Rule recovery can timeout if there is a high eps. You can modify the <code>rules.recovery.time-limit</code> property to set a higher recovery time limit to attempt to prevent this timeout so the server will not stop loading events from the database for checkpoint. The default value for <code>rules.recovery.time-limit</code> is 120 seconds (two minutes).</p> <p>However, the timeout can still occur even after you raise the time limit, due to overall system load, high eps, or a large number of rules.</p> <p>For details on editing the <code>server.properties</code> file, see the "Editing Properties Files" topic in the ESM Administrator's Guide.</p>
NGS-14585	<p>In some circumstances, the action of changing the operator from <code>'='</code> to <code>StartsWith</code> or <code>Contains</code>, and back again to <code>'='</code>, can erroneously apply an additional level of character-escaping to the string operand. This can then result in comparison against an operand string which is not the intended one, which was interpreted as a failure of <code>StartsWith</code> or <code>Contains</code>. Failure to remove additional character-escaping has been prevented.</p>

Issue	Description
NGS-14264	Sometimes Warning messages such as "Discarding current internal data structures to prevent overflow. Distinct values limit set to 1000" can be seen continuously in server.logs for data monitors. These messages can be ignored as it does not affect functionality
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.

## Analyze/Search

Issue	Description
NGS-8530	<p>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.</p> <p>Workaround: In the ACC search page, after a search is completed click Export. Instead of selecting the checkbox to include all fields, enter a comma-separated list of fields in the text area provided.</p>

## ArcSight Console

Issue	Description
NGS-17864	<p>On certain operating systems, show event details option on an eventID in a Query viewer does not show all event details like EventID, Start time, ManagerReceipt Time.</p> <p>Workaround: Open the event in an Active channel first and then view the event using Query viewer using Show Event Details. In some cases restart of the console also solves the issue</p>
NGS-17863	In an MSSP environment, under certain circumstances a tenant may notice event(s) which should match the user group's Access Control List settings for Events, but these events will be stuck in "Loading Event..." state within the Active Channel. Workaround: Add the "Customer Name" column to the Active Channel and the events will load successfully.
NGS-17855	In the Help > About menu on both the ArcSight Console and Command Center, the URL to HP ArcSight's copyrights, trademarks, and acknowledgements should be <a href="https://www.protect724.hpe.com/docs/DOC-13026">https://www.protect724.hpe.com/docs/DOC-13026</a> .

Issue	Description
NGS-16582	<p>When running an SQL query via 'arcdt' or using an ESM resource that produces an SQL query (for example, Active Channel, Query/Query Viewer, or Report), and the conditions of the SQL query contain some IP address constants either via 'IN()', or multiple '=' predicates, combined by 'OR' operators, the SQL query can produce incorrect results.</p> <p>Workaround:</p> <p>To apply the workaround on ESM CORRE:</p> <ol style="list-style-type: none"> <li>1. Edit the /opt/arcsight/logger/data/mysql/my.cnf file.</li> <li>2. Change the following parameter as following:</li> </ol> <p>from:</p> <pre>engine_condition_pushdown = 1</pre> <p>to:</p> <pre>engine_condition_pushdown = 0</pre> <ol style="list-style-type: none"> <li>3. Stop and restart all ESM services</li> </ol> <p>To roll back the workaround on ESM CORRE:</p> <ol style="list-style-type: none"> <li>1. Revert the change in the /opt/arcsight/logger/data/mysql/my.cnf</li> </ol> <p>from:</p> <pre>engine_condition_pushdown = 0</pre> <p>to:</p> <pre>engine_condition_pushdown = 1</pre> <ol style="list-style-type: none"> <li>2. Stop and restart all ESM services</li> </ol>
NGS-16105	<p>In the Package framework, SUBSET of AL/SL resources moved between groups, does not show correct move location after uninstall and reinstall.</p>
NGS-15686	<p>When using Logger Integration Commands, authentication on Logger 5.3 SP1 will fail when using password authentication.</p> <p>Workaround: Configure Logger and Integration Commands for one-time passwords.</p>
NGS-14853	<p>On Windows, when uninstalling the base build after P2 has already been uninstalled, after you run the uninstaller program and click Done, the system will restart automatically with no prompt to let you choose whether to restart the system or not.</p>
NGS-14227	<p>In a Non-English installation in the Console, if you create a case and then immediately select Add to Case/Case in Editor, the events may not be added to the newly created case.</p> <p>Workaround: Save and lock the new case before adding events to it.</p>



Issue	Description
NGS-14191	<p>When you run the Database Performance Statistics dashboard in an environment that has a local language other than English, you may see two sets of entries in the Database Free Space area: one in the local language used by ESM, and the other in English.</p> <p>If this happens, both the ArcSight Console and the ACC will be affected.</p>
NGS-14188	<p>ESM Console installation on non-English path in Windows machines fails to configure Console.</p> <p>Workaround: Use English filenames in installation paths. Or run Console configuration after installation finished by running the consolesetup script from Console ..\current\bin directory.</p>
NGS-14002	<p>If a report is run with a parameter on an annotation, the report result will be empty.</p>
NGS-13829	<p>Stages resources are erroneously not locked as system content and are editable from the ArcSight Console, on the resource Navigator &gt; 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-13125	<p>When creating reports, a custom parameter of type floating point, will result in an exception.</p>
NGS-11278	<p>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.</p> <p>In addition, the correct number of total cases is displayed in the upper right corner; however, the cases are not displayed in the channel.</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>"Cannot find sree properties in /home/arcsight/Console/current/reports/sree.properties."</p> <p>Workaround: Ignore this message.</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-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>

Issue	Description
NGS-7173	The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.
NGS-6800	Sometimes the legend for the /All Dashboards/ArcSight Administration/ESM/Content Management/Top Synchronization Errors dashboard component contains too many characters and the graph does not display.  Workaround: Run the individual report for the dashboard component.
NGS-5981	When annotating groups of events, the count of events which the Console indicates were updated may not reflect the correct number of updated event records.
NGS-3084	Global variable fields of the type "GetActiveList" are not displayed on custom layouts and image dashboards. This behavior is seen on custom layouts when using the ArcSight Console, and image dashboards when using ArcSight Web and ArcSight Command Center.  WorkAround: To view these fields correctly, use the standard layout on ArcSight Console.
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: Use the following two filters in AND condition.  EventAnnotationFlags Is NOT NULL  EventAnnotationFlags != 0

## ArcSight Manager

Issue	Description
ESM-51070	Connector statistics file to be processed correctly on Managers other than the primary destination Manager. Related content such as the rule Connector Discovered or Updated will be impacted.
ESM-48068	After asset auto-creation, if the manager does not restart and the server.std.log shows a message about a "conflicting device with the same hostname/ipaddress <resource id>", then two assets have the same resourceid. This conflict has to be resolved before starting the manager.
ESM-47625	When exporting a case or other resource, the Creation Time is changed to the time of the export.
ESM-46699	Updating a Trend by refreshing it works only once. Thereafter, the trend does not refresh with updated information.
ESM-30008	Installing an exported package from a bundle file occasionally results in the following error: Install Failed: Resource in broker is newer than modified resource.  Workaround: Re-import the package.

Issue	Description
NGS-17920	After running reports, the archive report folder name may have leading zero missing in the month number, for instance 2-16-2016. For workaround, customers need to add a property <code>report.datetime.dateFormat=MM-dd-yyyy</code> into <code>server.properties</code> and restart the Manager.
NGS-17190 NGS-17059	The situation reported by the MySQL log message "[ERROR] /opt/arcsight/logger/current/local/mysql/libexec/mysqld: Sort aborted" and the ESM server log message "Temporary sort space limit exceeded" can be addressed by increasing the value of <code>sort_temp_limit</code> in <code>my.cnf</code> .
NGS-14860	Multiple failure messages are generated in <code>logger_web.out.log</code> when stopping arcsight services.  These messages can be ignored.
NGS-14383	Archive Processing Report lists don't differentiate Archive Name for different Storage Groups.  Workaround: Use the <code>FilePath</code> field when working with Archive Audit Events.
NGS-14260	If some resource on the primary (for example, memory, or CPU) is temporarily exhausted, it may be necessary to reboot the primary to recover HA control completely. Symptoms during the resource exhaustion can include:  1. ESM running very slowly.  2. Cannot make a new SSH connection to the system.  ESM will run normally after the resource exhaustion ends. But the following continuing symptoms may be seen:  1. HA will not failover via <code>arcsight_cluster</code> prefer or <code>arcsight_cluster</code> offline.  2. HA may report that the resources "ESM", "Filesystem", and "Service IP" are Stopped, when they evidently are running normally.  If these symptoms are seen together, the primary system should be rebooted.
NGS-12358	A package resource may become out of sync with the content that has been added to the package. To workaround, recreate the package.
NGS-12105	The annotation stage name default value ('Queued') is displayed in the active channel, but this name does not display in the query viewer or in a report. Its other non-default value (for example, 'Initial', 'Follow-Up') is displayed correctly in the query viewer or report.
NGS-9734	In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.
NGS-9733	When logging in to the ArcSight Console, you could get an error related to logging in to core services. Login will still continue.

Issue	Description
NGS-9503	There is a possibility that small segments of data in the CORR-Engine may become corrupted. If a query attempts to access data that has become corrupted, the query will skip the corrupted data and log an error message in the MySQL log. This enables MySQL to continue and return a result on the data that is not corrupted.
NGS-9109	An incorrect OID is provided for ArcSight SNMP Trap. A third party package causes the OID for a trap to be translated incorrectly.
NGS-8926	<p>If there is a Forwarding Connector running between a source Manager and any destination, and a correlation event occurs on the source Manager,</p> <p>then the Forwarding Connector will forward the correlation event and its associated correlated events to the destination.</p> <p>However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database.</p> <p>As a result, if there is any correlation content on the source Manager looking for the value EventAnnotationFlags=correlated, the content will not be matched or triggered.</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 persist.
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 is not populated.</p> <p>Workaround: Re-import the same package.</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.</p>

## CORR-Engine

Issue	Description
NGS-14477	Space-based retention cleans up same day data, but even after increasing the space, the system does not recognize that the space has been increased until midnight.
NGS-14041	Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the "Ignore Case" option, which rely on the UPPER function.

Issue	Description
NGS-11080	When offline event archives are restored to another system using the restorearchives command, the event annotations are not restored. The offline archives are not affected.
NGS-4884	<p>It is possible to get no query result when querying the ArcSight.events table from arcdt or from mysql.</p> <p>If this occurs, execute the SQL using the command arcsight arcdt by following the steps below:</p> <ol style="list-style-type: none"> <li>1. Create a file such as 1.sql in /tmp/ containing this SQL: "select * from arcsight.events where arc_deviceHostName = 'host_name' limit 2;"</li> <li>2. Run arcdt tool and pass the created SQL file as parameter: -f /tmp/1.sql and the specified time frame assuming you have events for this time frame:  <pre>./arcsight arcdt runsql -f /tmp/1.sql -type EndTime -ss &lt;start time&gt; -se &lt;end time&gt;</pre> <p>Use start and end times in the form YYYY-MM-DD-HH-MM-SS-MSS-TZ, such as 2013-02-04-00-00-00-000-PST. (MSS is milliseconds.)</p> <p>More information about running this tool can be obtained by running tool with help option (arcsight arcdt help), or by referring to this command in the Administrator's Guide appendix, "Administrative Commands."</p> </li> </ol>
NGS-4790	<p>To resolve a "database full" condition, free up space in the ArcSight System Storage 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
NGS-17474	When a case is viewed in ACC, renamed and saved, now when user go back to cases resource browser case are being displayed in grid. User has to refresh the grid.
NGS-17407	In system has too many notifications, ACC will not show notification counts in notification view. So workaround is stop manager, Delete unused notifications such as undeliverable or old pending notifications and start manager.

Issue	Description
NGS-17385	Under certain circumstances, the notifications that get into Not Acknowledged state cannot be acknowledged neither from Console or ACC.
NGS-17344	If a query viewer in table view is not showing data in the ACC Navigator dashboard, set a refresh interval in console and save. When the dashboard reloads in the ACC the query viewer will show data.
NGS-16806	In an MSSP context, exporting search results using "Save to ArcSight Command Center" violates the separation between tenants within the system.  Workaround: To mitigate this by disabling the functionality, set <code>search.export.saveToServer.enabled=false</code> in <code>logger.properties</code> (as it is true by default/if absent).
NGS-14900	There is a rare case that may cause confusion in channel event data visualization screen. If the event interval is less than 1 minute apart. The depending charting library, d3.js, is not able to handle this minute rounding case. The issue will rarely occur in a production environment.
NGS-13926	The stages available in the ArcSight Console Stage drop-down list do not always display in the ACC active channel.  The stage "Follow-Up" is available in the ArcSight Console Annotation Stage drop-down list, but does not display in the Annotation Stage drop-down list in ACC active channel.
NGS-13854	If you are using other than an English installation, some dashboard pages may not load in the ACC. You can still access these pages through the ArcSight Console.
NGS-12968	The new date field global variable will not display date value correctly in ACC dashboards. For example, create a variable of this type :  Type Conversion -> Convert String to Date  WorkAround: Use this variable in two data monitors and add these data monitors to a dashboard. In the dashboard, one of the data monitor displays the date format correctly, but the other data monitor shows it as a long number.
NGS-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-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-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.
NGS-7907	When you perform peer search using IN operators for IP address, MAC address, or Enum fields, no results are returned and an error message is displayed.

Issue	Description
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>
NGS-7648	<p>The performance of peer search is slow in the current implementation.</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 = &lt;username&gt; will return an error while viewing cases of a case query group in any UI.</p> <p>Workaround: Use owner = &lt;user resource_id&gt; instead of owner = username.</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>
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, and can be ignored.</p>

Issue	Description
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-1283	<p>Non-administrator users cannot access the Users, Connectors, and 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, and Configuration page in ArcSight Command Center.</p>

## Connectors

Issue	Description
NGS-12742	<p>Event ID may appear as negative when using three or more forwarding connectors to a single destination. This can be ignored. A negative event can result because Java has only a signed 64 bit value, and in a multi-tier deployment that uses the higher 16 bit, event IDs may be presented as negative. For details, see the Event ID and Event Forwarding document, located at <a href="https://www.protect724.hpe.com/docs/DOC-12310">https://www.protect724.hpe.com/docs/DOC-12310</a>.</p>
NGS-12407	<p>Annotation flag indicating 'forwarded' may not get set when forwarding events from ESM 6.8.</p>
NGS-1423	<p>Upgrading a connector, running on Windows, 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-17370	<p>The second and subsequent Connected Hosts entries are ignored by High Availability. They will not be pinged to calculate Network status, and they will not be used by Failover-Check to determine if a failover should be done.</p>



Issue	Description
NGS-14337	<p>When ESM is set up in FIPS mode, an error like the following: "Couldn't get hostname from manager certificate: java.security.KeyStoreException: PKCS11 not found" may appear in the ServiceStatusChecker.log file after executing the "service arcsight_services status" command.</p> <p>This error can be ignored if no connection issues are observed between Console/ACC and the manager.</p>
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-6996	<p>There might be some data monitors disabled after the upgrade, while they are enabled in a fresh installation and vice versa.</p> <p>Workaround: Re-enable any data monitors that you want enabled after upgrade.</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-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-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>

Issue	Description
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.</p> <p>Workaround: Remove the No Events enforcing filter.</p>

## Localization

Issue	Description
NGS-16276	<p>Localized date/time format: this note applies to ESM deployed in a localized environment.</p> <p>If the property <code>report.datetime.dateFormat</code> in <code>server.properties</code> is defined, ESM uses its value as the format string, otherwise it uses the standard java method to obtain localized date format: <code>(DateFormat.getDateInstance(DateFormat.SHORT, DateFormat.DEFAULT))</code></p> <p>The change affects only the report parameters - not report data (table columns)</p> <p>You can modify the following parameters in <code>server.properties</code> to configure data format for their report.</p> <p># The date format for all report content</p> <p><code>report.content.dateFormat=dd MM yyyy HH:mm:ss</code></p> <p># The date format for datetime report parameters (e.g. <code>\$CurrentDateTime</code>, <code>\$Now</code>)</p> <p><code>report.datetime.dateFormat=dd-MM-yyyy-HH:mm:ss</code></p> <p># The date format for date report parameters (e.g. <code>\$CurrentDate</code>)</p> <p><code>report.date.dateFormat=dd-MM-yyyy</code></p> <p># The date format for month type report parameters (e.g. <code>\$CurrentMonth</code>)</p> <p><code>report.month.dateFormat=MM-yyyy</code></p> <p># The date format for week type report parameters (e.g. <code>\$CurrentWeek</code>)</p> <p><code>report.week.dateFormat=ww-yyyy</code></p>

Issue	Description
NGS-10687	<p>If the property(<code>report.datetime.dateFormat</code> ) in <code>server.properties</code> is defined, the value is used as the format string. Otherwise, standard Java is used to get the localized date format (<code>DateFormat.getDateTimeInstance(DateFormat.SHORT, DateFormat.DEFAULT)</code>).</p> <p>The change affects only the report parameters - not report data (table columns)</p> <p>User can modify the followings in <code>server.properties</code> to configure data format for their report.</p> <p># The date format for all report content</p> <pre>report.content.dateFormat=dd MM yyyy HH:mm:ss</pre> <p># The date format for datetime report parameters (e.g. <code>\$CurrentDateTime</code>, <code>\$Now</code>)</p> <pre>report.datetime.dateFormat=dd-MM-yyyy-HH:mm:ss</pre> <p># The date format for date report parameters (e.g. <code>\$CurrentDate</code>)</p> <pre>report.date.dateFormat=dd-MM-yyyy</pre> <p># The date format for month type report parameters (e.g. <code>\$CurrentMonth</code>)</p> <pre>report.month.dateFormat=MM-yyyy</pre> <p># The date format for week type report parameters (e.g. <code>\$CurrentWeek</code>)</p> <pre>report.week.dateFormat=ww-yyyy</pre>

## SmartConnectors

Issue	Description
NGS-13049	When upgrading the forwarding connector, two fatal exception messages will appear, regarding <code>[agents[0].arcsightuser]</code> and <code>[agents[0].arcsightpassword]</code> . These messages may be safely ignored.

## Fixed Issues

The following issues are fixed in this release.

## Analytics

Issue	Description
NGS-16258	Due to a date formatting issue, the start time of a query range can sometimes (infrequently) end up greater the end time, resulting in SQL returning no data from the query. If this happens, because it is infrequent, re-running the query (refreshing the trend) will almost always correct the problem.

Issue	Description
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).</p> <p>This issue is now fixed.</p>

## ArcSight Console

Issue	Description
NGS-14299	<p>In Advanced Editor for InGroup operator, for an asset, select only an asset or asset category. Selecting a zone will not retrieve any information as an asset does not have a relationship with a zone group. This is for both Console and the ArcSight Command Center.</p> <p>This issue is now fixed.</p>
NGS-13910	<p>In the data monitor, /All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/CPU Sensors might have no data, because the audit events from Logger changed.</p> <p>This issue is now fixed.</p>
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.</p> <p>This issue is now fixed.</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> <p>This issue is now fixed.</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-146	<p>In some cases, event-based Active Channels that include an InCase filtering condition did not display events that belong to a case but were 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 was unable to find and display such events correctly after the partition is archived.</p> <p>This issue is now fixed.</p>

## ArcSight Manager

Issue	Description
NGS-16170	<p>Importing a CSV file into an active list with entries with the characters \n, \b, \t, \r (for example, C:\users\requests) could cause the characters to appear erroneously in the ESM active list entry (for example, C:\users\requests displays as C:\usersequests). Also, when this data was exported into a csv file, the data displayed incorrectly (\n causes a newline space in the csv data).</p> <p>This issue is now fixed.</p>
NGS-14293	<p>The current version of ESM API (version 1.0) returns large negative numbers for NULL database fields. Depending on field type that would be either -2147483648 (Integer.MIN_VALUE), -9223372036854775808 (Long.MIN_VALUE) or 5e-324 (Double.MIN_VALUE).</p> <p>All such fields in returned Resource or Event representations should be treated as NULL fields.</p>
NGS-11730	<p>Shutting down services by using the arcsight_services command might result in exceptions in the log file.</p> <p>This issue is now fixed.</p>
NGS-11291	<p>For non-admin users, if the filter refers the field which is neither basic (or required) field nor shown field in Active Channel, the events matching the filter were indicated on active channel with the message "Loading Event... ID:", but the events did not actually load.</p> <p>(Note that for a non-admin user to open a channel in ACC, permissions to the resource on which the filter is created must be added for that user group.)</p> <p>This issue is now fixed.</p>
NGS-8285	<p>Services could fail to stop after running "/etc/init.d/arcsight_service stop" or "/etc/init.d/arcsight_service stop all".</p> <p>This issue is now fixed.</p>
NGS-5271	<p>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.</p>

## CORR-Engine

Issue	Description
NGS-13993	<p>When several Managers were forwarding to the same destination, read performance could be impacted on the destination Manager due to an issue related to the forwarded event id. Channel, query viewer, trend, and report performance could be impacted when the forwarded event ID was negative.</p> <p>This issue is now fixed.</p>

## Command Center

Issue	Description
NGS-15443	<p>The Event Throughput data monitor on the Event Throughput dashboard does not render properly. This issue can appear intermittently.</p> <p>This issue is now fixed.</p>
NGS-14923	<p>On Windows Server 2012 R2, CAC PIN request dialogs can cause IE and Chrome browsers to stop working. This occurs when ActivClient middleware is used.</p> <p>This issue is now fixed.</p>
NGS-14311	<p>While configuring an existing filter condition of a channel, if the condition is "true" only, remove the "true" condition first before adding any other conditions.</p> <p>This issue is now fixed.</p>
NGS-14230	<p>Visualization of variable fields is not supported.</p> <p>This issue is now fixed.</p>
NGS-13895	<p>Type values should be in upper case in the ArcSight Console; were shown in lower case.</p> <p>This issue is now fixed.</p>
NGS-13800	<p>In the Advanced Editor for the InGroup operator for an asset, select only an asset or asset category. Selecting a zone will not retrieve any information as an asset does not have a relationship with a zone group. This applies to both the Console and the ArcSight Command Center.</p> <p>This issue is now fixed.</p>
NGS-12984	<p>Channels in ACC did not support concentrator agent field.</p> <p>This issue is now fixed.</p>

Issue	Description
NGS-11143	<p>In visualization user interface, when there is an attempt to investigate fields with no values, the condition was set incorrectly. As a result, channel did not show any events.</p> <p>This issue is now fixed.</p>
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 5-10 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-10634	<p>The condition summary might not display completely in the condition summary window.</p> <p>This issue is now fixed.</p>
NGS-9192	<p>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.</p> <p>The filter definition is now parsed as shown in the ArcSight Console.</p> <p>The issue is now fixed.</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>This issue is now fixed.</p>

## Configuration

Issue	Description
NGS-10800	<p>An error like the following will appear in the logger logs during logger startup:</p> <p>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)</p> <p>This will not cause any issue and can be safely ignored.</p>

## Installation and Upgrade

Issue	Description
NGS-11267	<p>If you have customized the property file <code>/opt/arc sight/manager/config/server.wrapper.conf</code> in your source manager, during upgrade, the customized properties are not transferred to the upgraded manager location.</p> <p>This issue is now fixed.</p>
NGS-10147	<p>After installing the ArcSight Core package, the package view may show some resources displayed in red strike-through text. These resources are excluded in the package on purpose, and can be safely ignored.</p>
NGS-10069	<p>Previously, the upgrade script assumed that the password for both ArcSight and MySQL were the same password.</p> <p>This issue is now fixed and these passwords can be different.</p>
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 <code>database.configuration.log</code> file: <code>"java.lang.NoClassDefFoundError: Could not initialize class sun.awt.X11GraphicsEnvironment"</code>.</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>



# Send Documentation Feedback

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

## **Feedback on Release Notes (ESM 6.9.1c)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!