

Release Notes

ArcSight ESM 6.5c SP1

April 22, 2014



Copyright © 2014 Hewlett-Packard Development Company, L.P.

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

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

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

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

Contact Information

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

Revision History

Date	Product Version	Description
4/22/2014	HP ArcSight ESM 6.5c SP1	Release Notes

..

Contents

ArcSight ESM 6.5c SP1	5
Welcome to ESM 6.5c SP1	5
What's New in This Release	5
Upgrade and Migration Support	8
Geographical Information Update	8
Vulnerability Updates	8
Verifying Secure Delivery	9
Usage Notes	9
Restoring my.cnf Customizations	9
Cases UI Customizations after Upgrade	9
Domains	9
Running Concurrent Searches	10
Starting and Stopping Components	10
Issue When Subscriber is Added As a Peer	10
Discover Fields List - Top Values and Values by Time	10
Path Change for arcsight_services Command	10
Frequently Asked Questions about ESM with CORR-Engine	11
Fixed Issues in ESM 6.5c SP1	13
Analytics	13
ArcSight Console	14
Command Center	14
General	15
Open Issues in ESM 6.5c SP1	15
Analytics	15
Analyze/Search	16
ArcSight Console	17
ArcSight Manager	19
CORR-Engine	21
Command Center	21
Connectors	25
General	25
Installation and Upgrade	26
Pattern Discovery	27

ArcSight ESM 6.5c SP1

These release notes discuss the following topics.

["Welcome to ESM 6.5c SP1" on page 5](#)
["What's New in This Release" on page 5](#)
["Upgrade and Migration Support" on page 8](#)
["Geographical Information Update" on page 8](#)
["Vulnerability Updates" on page 8](#)
["Verifying Secure Delivery" on page 9](#)
["Usage Notes" on page 9](#)
["Frequently Asked Questions about ESM with CORR-Engine" on page 11](#)
["Fixed Issues in ESM 6.5c SP1" on page 13](#)
["Open Issues in ESM 6.5c SP1" on page 15](#)

Welcome to ESM 6.5c SP1

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 topic describes the new features and enhancements added in ESM 6.5c SP1.



Case Management Enhancements

This release includes the following enhancements to the case management feature:

- **Ability to search the Notes tab**

You can now search content in cases' Notes tab. This enhancement is not limited to the Case resource but also applies to all resources that have the Notes tab.

Refer to the "Finding Resources" topic in the ArcSight Console User's Guide's section on Managing Resources. This topic includes a discussion on how to escape special characters in your search fields. This feature is supported only on the ArcSight Console.

■ **Permission to delete cases**

In new ESM installations, users you add to groups under Custom User Groups will require permission before they can delete cases. You can control a custom user group's ability to delete cases based on the new ACL operation permission, `/All Permissions/ArcSight System/Case Operations/Case Delete`. If a particular custom user group does not have this operation permission, the right-click menu option, `Delete Case`, is disabled for users in that group.

User groups under Administrators and Default User Groups automatically have the permission to delete cases. If a user belongs to two groups, and one group has permission to delete cases but the other group has not, the ability to delete cases takes precedence.

If you upgraded from an older ESM version, all default and custom user groups automatically keep their legacy permission to delete cases.

For details about deleting cases, refer to "Case Management and Queries" in the ArcSight Console User's Guide or "Cases" in the ArcSight Command Center User's Guide.

For details about ACL permission settings for user groups, refer to "Managing Users and Permissions" in ArcSight Console User's Guide or "Edit Advanced Permissions" in the ArcSight Command Center User's Guide.

■ **Preserving deleted cases**

In this release, you can preserve view-only snapshots of deleted cases for historical purposes. This feature requires a new property setting, `case.archive_ondelate.enabled=true`

Deleted cases are stored in the Manager's `archive/cases` directory. For details on the behavior of deleted cases, refer to "Deleting a Case" in "Case Management and Queries" in the ArcSight Console User's Guide or "Cases" in the ArcSight Command Center User's Guide.

For details on property setting, refer to "Managing and Setting Properties File Settings" in the ESM Administrator's Guide.

■ **Ability to mark case attribute fields as mandatory**

Previously, only the **Name** field was required. In this release, you can specify which case fields are mandatory for your business. The changes are seen on both ArcSight Console and ArcSight Command Center. If you view cases after fields have been specified as mandatory, you will not be able to close the case editor without entering values in the new mandatory fields.

Note: A rule that creates or updates a case does not check for mandatory fields, although the rule will still fire successfully. For new cases, you can optionally make the rule set the mandatory fields; or manually set the mandatory fields by opening the created case later. For cases being updated, the rule uses existing values unless you specify different values. For details on creating rules and using the Add to Case rule action, refer to "Rules Authoring" in the Command Center User's Guide.

If you want to customize the Case Editor UI, contact HP Professional Services for ArcSight products.

■ **Copying event data from one case to another**

You can copy event data directly from one case to another. The events continue to exist in the destination case even after the source case is deleted. This feature is supported only on ArcSight Console, and works only within the same ESM installation.

For details, refer to "Copying Event Details from Case to Case" under the "Case Management and Queries" section of ArcSight Console User's Guide.

■ Ability to run a case report

You can now create a simple case report in one of these output formats: PDF, XLS, RTF, CSV, or HTML. The output consists of two columns: the first column displays the case attribute's name and the second column, the corresponding attribute value. You have the option to send the generated report to email recipients. The report and underlying query have been predefined for you (see related information, [Case Query and Report in Standard Content](#)). This feature is supported only on the ArcSight Console.

For information, refer to "Creating a Report from a Case" under the "Case Management and Queries" section of ArcSight Console User's Guide.

■ Enhanced audit trail of case modifications

Case audit events have been enhanced so that you can track case modifications when a case is re-assigned to a different owner, and that new owner has made changes. You can view a single case's audit trail on the case's Notes tab, or create an event viewer to investigate multiple events. This feature is supported only on the ArcSight Console.

For more information, refer to "Tracking Modifications to a Case" under the "Case Management and Queries" section of ArcSight Console User's Guide.

■ Audit trail sort order

The audit trail on a cases Notes tab are now sorted in chronological order.



Notifications

You can now delete informational messages on the ArcSight Console and ArcSight Command Center.

Refer to "Deleting Informational Notifications" under the "Managing Notifications" section of ArcSight Console User's Guide and "My Notifications" under the "The Home Page" section of the ArcSight Command Center User's Guide.



Case Query and Report in Standard Content

A standard report, `/All Reports/ArcSight System/Core/Selected Case Report`, and its underlying query, `/All Queries/ArcSight System Core/Selected Case Report/Selected Case Query`, are provided to support the feature to create a basic report on a case. You can use the report as is, or customize it by adding more fields to the basic report.

For information, refer to "Creating a Report from a Case" under the "Case Management and Queries" section of the ArcSight Console User's Guide.



Platform Support

ESM 6.5c SP1 adds SUSE Linux Enterprise 11 SP3 (64-bit) to the list of supported platforms. Refer to the Product Lifecycle Document for a complete list of supported platforms and versions.



Addresses critical issues in ESM 6.5c

Under certain loads, an unstable condition can on occasion arise that leads to a Signal 11 occurrence. This service pack provides a significant improvement to reduce the likelihood of a Signal 11 condition.



Geographical Information and Vulnerability Mapping

This service pack provides a [Geographical Information Update](#) and [Vulnerability Updates](#).

Upgrade and Migration Support

The following upgrade paths are supported for this release:

- ESM 6.5c to ESM 6.5c SP1
- ESM 6.5c Patch 1 (or greater) to ESM 6.5c SP1

For details, refer to the Upgrade Guide for ESM 6.5c to 6.5c SP1.

The following migration paths are supported for this release:

- ESM v5.5 to v6.5c SP1
- ESM v5.5 Patch 1 (or greater) to v6.5c SP1

For details, refer to the Migrating ESM Resources From Oracle to CORR-Engine for ESM 5.5 P1 to ESM 6.5c SP1.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20140301.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU-1066 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Enterasys Dragon IDS updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S776 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2352 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
McAfee Intrushield updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, MSKB
TippingPoint UnityOne DV8536 updated	Faultline, Bugtraq, CVE, Nessus, MSSB
ISS SiteProtector updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, MSSB, CERT
Symantec Endpoint Protection updated	Faultline, Bugtraq, CVE, X-Force, Nessus
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	CVE

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

Restoring my.cnf Customizations

If you have customised the file `/opt/arcsight/logger/data/mysql/my.cnf`, then before you upgrade, make a backup copy of it. The upgrade overwrites this file. After the upgrade, restore your customizations from the backed up version by comparing the two and adding your customizations to the upgrade's new version. Doing it this way helps preserve any improvements added in the new version.

Cases UI Customizations after Upgrade

If you customized the Cases UI on the existing 6.x environment, the customizations are not copied over automatically during the upgrade. The upgrade creates backups of several files and places them in `preUpgradeBackup` folders. Most of these are restored correctly after the upgrade; in this release a few are not. The workaround is to restore them manually after the upgrade as follows:

- 1** Copy `label_strings_en.properties` and `resource_strings_en.properties` under `/opt/arcsight/manager.preUpgradeBackup/i18n/common` to `/opt/arcsight/manager/i18n/common`.



For English, if the `*_en.properties` file does not exist under `/opt/arcsight/manager.preUpgradeBackup/i18n/common`, copy the `*.properties` file. If it exists, copy `*_en.properties`. For other locales, copy the `*_<locale>.properties` file.

- 2** Copy `caseui.xml` under `/opt/arcsight/manager.preUpgradeBackup/config` to `/opt/arcsight/manager/config`.
- 3** If a customized case details mapping to audit events exists, copy `case.properties` under `/opt/arcsight/manager.preUpgradeBackup/config/audit` to `/opt/arcsight/manager/config/audit`.
- 4** Restart the Manager for these changes to take effect.

Domains

The Domains feature is not supported for this release.

Running Concurrent Searches

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

Starting and Stopping Components



The commands for starting and stopping components in ESM 6.5c SP1 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 SP1, 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*:

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

If you inadvertently run unsupported scripts, rebooting the system restores 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 SP1. If you search the latest version of peer Logger using the ArcSight Command Center search feature, and you check both the Field Summary and Discover Fields options, the "Values by time" link in the pop-up for any field in the "Discovered Fields" list does not work.

Workaround: To use the Discover Fields option, run the search from the peer Logger.

Path Change for arcsight_services Command

On SUSE Linux, non-root users are not permitted to run commands from */sbin*. Therefore, we have changed the path for all users, regardless of operating system. To run the *arcsight_services* command as user *arcsight*, use

```
/etc/init.d/arcsight_services <command>
```

For example, run:

```
/etc/init.d/arcsight_services status all
```

instead of:

```
/sbin/service arcsight_services status all
```

All commands run by user *arcsight* now specify `/etc/init.d/`.

Note that in the online help system, the Administrator's Guide has a topic called "ArcSight_Services Command" in Appendix A, "Administrative Commands" that still refers to the `sbin` path. (The PDF of the Administrator's Guide is correct.) Wherever you see `/sbin/service arcsight_services use /etc/init.d/arcsight_services`.

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 SP1? What platform is ESM 6.5c SP1 supported on?

The ESM Manager and CORR-Engine components come integrated in a suite that is installed on a single machine. A single-machine installation provides better scalability with localized processing and storage tiers. ESM 6.5c SP1 should be installed on a single machine running one of these 64-bit operating systems: Red Hat Enterprise Linux 6.4, Red Hat Enterprise Linux 6.5, or SUSE Linux Enterprise 11 SP3.

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

The ESM 6.5c SP1 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 SP1?

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

Can ESM 6.5c SP1 be part of a mixed hierarchical architecture with ESM 5.x using a Forwarding Connector?

Yes. You can forward events from ESM 5.5 with latest patch to ESM 6.5c SP1. However, we recommend that you do not send events to ESM 5.5, and instead send them directly to ESM 6.5c SP1.

Will existing licenses work?

If you have a valid existing ESM license, you can use it with ESM 6.5c SP1.

Can I continue to use my existing Loggers with ESM 6.5c SP1?

Yes. You can forward events from Logger 5.5 with the latest patch to ESM 6.5c SP1 and vice versa.

Can I upgrade my existing ESM installation to ESM 6.5c SP1?

See ["Upgrade and Migration Support" on page 8](#)

How do I access 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 back up and restore my data in ESM 6.5c SP1?

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

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

Install ESM 6.5c SP1 first. Once you have installed the ESM 6.5c SP1 software, you can migrate your resources from a legacy ESM 5.x installation. See ["Upgrade and Migration 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 6.5c SP1 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. 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 correlated base events is not supported.
- Daily partitioning on trend and session list data is replaced by weekly partition.

Fixed Issues in ESM 6.5c SP1

Analytics

Issue	Description
NGS-8579 NGS-7906	In a Query, the GetHour variable returned 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. This is now fixed.
NGS-8411	In some cases the values of some variables (group functions) in a report did not match their preview values. This is now fixed.
NGS-8114	Once a rule got disabled due to too many firings, it would continue getting disabled even without new firings because the calculation of #firings/minute does not get reset properly. This has been fixed in this release.
NGS-7876	If the ConvertStringToList variable function was used in any resources prior to upgrading to 6.5c, those resources were broken after the upgrade, and the variables (local or global) displayed as empty definitions in the editor. This is fixed in 6.5 SP1. Now they are correctly displayed after the upgrade.
NGS-7865	A rule was marked invalid if it contained a condition using the ContainsValue operator. Now the ContainsValue operator no longer makes a rule invalid.
NGS-7174	Some audit events' severities were showing incorrect values after session expired. This has been fixed in this release.
NGS-6521	The Day function now converts timestamp data correctly. For the event count history, the Event Count Last 7 Days query viewer now shows the correct data.

Issue	Description
NGS-5643	<p>If you queried cases with the condition, Owner = <the user's name>, the query failed because it was expecting the owner's Resource ID.</p> <p>This is now fixed. If you query a case for the owner, you can either use the owner's Resource ID or the owner's name.</p>
NGS-4184	<p>If a rule contains multiple negated event aliases with timeout values specified, the rule does not trigger until the sum of the timeout values has elapsed. For example, consider a rule with three event aliases: event1 is positive, event2 is negated with timeout = 1 minute, and event3 is negated with timeout = 2 minutes. The rule does not trigger until at least 3 minutes after event1 has been matched. Moreover, if the event expiration time (by default the aggregation time window) is only 2 minutes, the rule does not trigger at all because event1 will be removed from memory prior to the cumulative timeout.</p> <p>Workaround: We recommend that you specify a positive timeout value for only one negated alias, and set the remaining timeouts to zero.</p> <p>This is documented in the "Negating Event Conditions" topic in the "Rules Authoring" section of the ArcSight Console User's Guide.</p>

ArcSight Console

Issue	Description
NGS-8282	<p>Previously, there was no way to clear, delete, or remove informational notifications displayed on the Informational tab of the Console's Notifications panel. This issue is now fixed. The Informational tab has a Delete button. To delete informational notifications, click the Notifications icon on the Console toolbar, click the Informational subtab, select the informational notification you want to delete, and click the Delete button. Then confirm the deletion.</p>
NGS-8155	<p>There was an issue in ESM 6.5c in which the Trend Data Viewer displayed partial data on the trend runs. This is fixed. Users are now able to view up to 2000 trend entries in the Trend Data Viewer.</p>
NGS-7997	<p>On the Case Editor's Notes Tab, if you entered foreign language special characters such as Russian, German, or Portuguese, ESM added them in an unreadable encoding. This is now fixed.</p>

Command Center

Issue	Description
NGS-8378	<p>On the search page of the Command Center in ESM 6.5c, there was a message, "Database fragmentation detected. Run Database Defragmentation under the Configuration - System Maintenance Menu." There is no database defragmentation function and this message no longer appears.</p>
NGS-7833	<p>Previously, if you used any search pipeline operators that created new fields or selected fields that were not in the default field set, these selected fields would not be displayed in the search results.</p> <p>Now the results show any user-defined fields in addition to the seven default fields (*user, sourceAddress, destinationAddress, priority, deviceVendor, deviceProduct, and Raw Message).</p>

General

Issue	Description
NGS-8263	Under certain loads, an unstable condition could on occasion arise that leads to a Signal 11 occurrence. This service pack provides a significant improvement to reduce the likelihood of a Signal 11 condition.
NGS-6790	Asset global variables with group functions did not work in reports and active channels. Reports with such functions would not always complete and such global variables would return null in the active channel. This is now fixed.

Open Issues in ESM 6.5c SP1

Analytics

Issue	Description
ESM-49283	When defining filters, for a hostname to be properly interpreted from the Request URL, the host name needs to be enclosed either within // (double slash) and / (single slash); or within // (double slash) and : (colon). For example: <code>https://<hostname>:8443</code> Such an event is retrieved correctly with the 'Request Url Host Is Not Null' filter. Don't use a filter with a condition that says 'Request Url Host != Null' because != makes the filter invalid.
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-29633	Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid. Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (for example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.
NGS-7896	Some rules under /All Rules/ArcSight Core Security can get triggered twice, because they are linked to other packages (for example, when the Intrusion Monitoring Foundation is installed). Workaround: Remove one of the links from the Real-Time Rules group.

Issue	Description
NGS-7181	Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.
NGS-6509	If you have the IdentityView 2.5 solution and have 500 K actors, the actor channels are not being loaded. This happens intermittently.
NGS-5756	From within a Query Viewer drill down for Active Channel, you cannot drill down to Field Set having IP address as part of Global Variable.
NGS-4187	<p>Trend tables that exceed 1 GB may cause a signal 11 error in the CORR-Engine.</p> <p>Workaround: Keep trend tables small (< 1G). Trends running on ESM with Oracle were often created to provide improved report performance on a subset of columns. This is no longer needed with CORR-Engine.</p> <p>The best way to reduce an overgrown trend table is to edit the trend and reduce the "retention" period. For the change to take effect, rerun the trend. If the trend data is no longer needed, you can delete the trend and the space that was used by the trend gets freed up.</p>

Analyze/Search

Issue	Description
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>
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"> - To on/off the multiline support search.multiline.fields.supported=true - To on/off the \\n and \\t support search.double.backslash.newlines.supported=false - 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
LOG-7046	<p>The time displayed on the histogram might not match the event time. This can happen when the /etc/localtime file is not symbolically linked to the correct time zone.</p> <p>Workaround: Make sure that the /etc/localtime file is symbolically linked to the correct time zone in the /usr/share/zoneinfo file as shown in the following example. Then, restart the system.</p> <pre>sudo ln -s /usr/share/zoneinfo/<timezone> /etc/localtime</pre>

Issue	Description
LOG-6965	<p>When the time change due to Daylight Savings Time (DST) takes place, the following issues are observed:</p> <ul style="list-style-type: none"> - The 1 a.m. to 2 a.m. time period is represented in DST as well as standard time on the histogram. - The histogram displays no events from 1 a.m. to 2 a.m. DST even though the Logger received events during that time period. - 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. - 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. - 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. <p>Workaround: To ensure that all events are returned, specify an end time of 2:00:01 or later.</p>
LOG-5181	<p>Search results are not highlighted when there are multiple values that match the IN operator in a query.</p> <p>Workaround: None at this time. Highlighting works if there is only one item in the square brackets. As soon as there is more than one, no highlighting occurs.</p>

ArcSight Console

Issue	Description
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-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>

Issue	Description
ESM-39980	The Console can become unresponsive if you access other resources while building category models with a large number of actors.
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 the "Add to Existing Case" rule action in the Rule editor. This is because the resource selector only shows leaf nodes when there are less than 1000 cases in a group. This happens for all resources.</p> <p>Workaround: Arrange the resource hierarchy so there are no more than 1000 resources in a single group. Alternatively, use a dynamic case name (a case name that includes a variable) in your rule action to specify the case. In the ArcSight Console User's guide, search for "Dynamic case name" in the "Rules Authoring" chapter.</p>
ESM-36055	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.
NGS-8025	Stages resources are erroneously not locked as system content and are editable from the ArcSight Console, on the resource Navigator > Stages resource tree. Do not customize or move these stages resources, as doing so might cause the Manager to become unusable. The system content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.
NGS-7735	An overlapping session list contains duplicate entries for the same key field. The session list is part of variable definition and used in filter. If the filter is used in active channel and the session list entry is deleted, the deleted entry may continue to be displayed on the active channel. This condition is temporary and eventually the channel will be updated.
NGS-7526	Non-admin users need to have read permission manually added to /All Trends/ArcSight Core Security for Default User group.
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-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.

Issue	Description
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-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 an InCase filtering condition do not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit. Case-related events are copied to a special table so they can remain available after being archived, but the channel is unable to find and display such events correctly after the partition is archived. Workaround: Use the case event editor or Reports, which can correctly find and display these events.

ArcSight Manager

Issue	Description
ESM-47625	When exporting a case or other resource, the Creation Time is changed to the time of the export.
ESM-41331	After the resource validation process is run, assets that are actually invalid appear to be valid. Workaround: To produce a correct report, run the resource validation script manually as follows: 1. Run the script using "arcsight resvalidate." 2. Run the script again using "arcsight resvalidate -persist false." 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.
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.

Issue	Description
ESM-37488	<p>Exporting a large active list with 10 million entries, or exporting rules that use such active lists, results in an exception in the server.std.log file. Additionally, the Manager runs out of memory and automatically restarts itself.</p> <p>Workaround: Use the export format instead of the default format while exporting the rule or active list definition using an archive or a package. This will not export the active list data.</p>
ESM-30008	<p>Installing an exported package from a bundle file occasionally results in the following error:</p> <p>Install Failed: Resource in broker is newer than modified resource.</p> <p>Workaround: Re-import the package.</p>
NGS-8573	<p>If case customization was done on the existing 6.x environment prior to 6.5c SP1 upgrade, the customizations are not copied over automatically during upgrade. It affects both manager and ArcSight Command Center.</p> <p>As a workaround, copy the following files which had customizations prior to upgrade to the current upgraded locations:</p> <ol style="list-style-type: none"> 1. Copy label_strings_en.properties and resource_strings_en.properties under /opt/arcsight/manager.preUpgradeBackup/i18n/common to /opt/arcsight/manager/i18n/common. <p>Note: For English, if the *_en.properties file does not exist under /opt/arcsight/manager.preUpgradeBackup/i18n/common, copy the *.properties file. If it exists, copy *_en.properties. For other locales, copy the *_{locale}.properties file.</p> <ol style="list-style-type: none"> 2. Copy caseui.xml under /opt/arcsight/manager.preUpgradeBackup/config to /opt/arcsight/manager/config. 3. If customized case details mapping to audit events exists, copy case.properties under /opt/arcsight/manager.preUpgradeBackup/config/audit to /opt/arcsight/manager/config/audit. <p>Restart the Manager for these changes to take effect.</p>
NGS-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>
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>

Issue	Description
NGS-1937	The Archive tool occasionally fails to import entries into an active list due to transient errors. In such situations, you might not see any errors, but the list does not get populated. Workaround: Re-import the same package.
NGS-1449	Shutting down services by using the <code>arcsight_services</code> 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.
NGS-172	Base events are not automatically annotated after rules trigger. Workaround: Set <code>logger.base-event-annotation.enabled=true</code> in <code>server.properties</code> and annotate the events manually.

CORR-Engine

Issue	Description
NGS-4790	To resolve a "database full" condition, you can free up space by doing the following: <ol style="list-style-type: none"> 1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend. 2. Reduce the retention period of specific trends. By default, trends retain 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time the trend runs. 3. Examine the contents of your session lists. Data is not usually removed from session lists. Running "<code>bin/arcsight dropSLPartitions -h</code>" will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.

Command Center

Issue	Description
LOG-12033	Pipeline searches for IP address fields do not display the results correctly. Workaround: When running pipeline searches for IP addresses, use field's Display Name; do not use the CEF name. 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. For the chart operator, do not use functions like <code>avg()</code> , <code>min()</code> , <code>max()</code> etc. Do not use the operators <code>eval</code> , <code>replace</code> , <code>rex</code> , and <code>regex</code> on IP address fields.
LOG-12032	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. ... chart sum bytesIn by deviceEventClassId span=5m Workaround: If you receive this error message, check your query, and add parenthesis if needed, as in the following example. ... chart sum(bytesIn) by deviceEventClassId span=5m

Issue	Description
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 ">=", "=", or "<=" to search IPv6 fields do not return the correct results.</p> <p>Workaround: When searching IPv6 fields, write your search to avoid using the "where" condition.</p>
NGS-8762	<p>In a rare case, when the search is completed, the hit count shown in the top part of the search results may not match the number shown in the table/grid's tool bar.</p> <p>Workaround: Since this can be caused by the timing of retrieving the search statistics, try to search again.</p>
NGS-8733	<p>Currently the ArcSight Command Center search ignores events with a NULL value in the field you are searching for, unless you specifically add NULL values (IS NULL) to the search criteria. For example, searching for a sourceAddress that is NOT InSubnet would ignore NULL source Addresses.</p> <p>The workaround is either search them through the ArcSight Console or ArcSight Web, or change such a query in ArcSight Command Center to add the condition "sourceAddress IS NULL" and use "or" to concatenate the condition to the original condition.</p> <p>For example:</p> <p>NOT sourceAddress InSubnet "10.*.*.*"</p> <p>should be queried as:</p> <p>sourceAddress IS NULL OR NOT sourceAddress InSubnet "10.*.*.*"</p>
NGS-7912	<p>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.</p>
NGS-7907	<p>When user perform peer search using IN operators for IP address, MAC address, or Enum fields, no results are returned and an error message is displayed.</p> <p>Workaround: None at this time.</p>
NGS-7891	<p>In Command Center Search, queries using some operators, such as chart, eval, rename, replace, rex, and regex, may not return the correct results when searching the following types of fields.</p> <p>IPv4 fields such as sourceAddress, MAC address fields such as destinationMacAddress, IPv6 fields such as dvc_custom_ipv6_address1, Geo Location fields such as: dest_geo_latitude, as well as the agentSeverity and locality fields.</p> <p>For example the following queries may not return the correct results:</p> <p>... chart max(agentSeverity) by name</p> <p>... chart max(dest_geo_longitude) by name</p> <p>... replace Low with notToWorry in agentSeverity</p> <p>... replace Local with localevents in locality</p> <p>Workaround: None at this time.</p>

Issue	Description
NGS-7861	<p>When using Internet Explorer 10, nodes in the Event Graph Data Monitor are not displayed properly when viewed in ACC-Dashboards.</p> <p>Workaround: Use Firefox or Chrome to view Event Graph Data Monitor properly.</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	<p>A condition in a Case Query Group with owner = <username> will return an error while viewing cases of a case query group in any UI. Workaround: Use owner = <user resource_id> instead of owner = username.</p>
NGS-7570	<p>When running very large report, 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	<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-7315	<p>If you delete a permission and then re-add the same permission and save it, the added permission is NOT saved.</p> <p>Workaround: After deleting a permission, save before re-adding or adding any permissions.</p>
NGS-7079	<p>If your environment contains more than 10,000 cases in one single group, displaying them in ArcSight Command Center might be very slow.</p> <p>Workaround: Avoid accumulating a large number of cases in one single group of your system. If your system contains more than 10,000 cases in one single group, display them in the ArcSight Console rather than Command Center.</p>
NGS-6933	<p>On upgraded systems, 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> <p>/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/Current Connector Status</p>
NGS-6896	<p>In the Chrome browser, the Select Resource drop-down sometimes doesn't work properly.</p> <p>Workaround: If this occurs, refresh the page to restore the content. Alternatively, use another browser.</p>
NGS-6886	<p>When a system has several peers and a peer stops responding, some pages in the ArcSight Command Center user interface might become slow to display. The delay happens regardless of the reason the peer system stopped responding.</p> <p>Workaround: Identify the peer that is not responding and remove its peer relationship on the Administration > Peers page, Peer Configuration tab. You can re-add the Peer later, when it is back in service.</p>
NGS-6812	<p>The ESM server log and the Logger server log may contain messages that say "...NotSerializableException: ...PeerLoggerRequestDestination".</p> <p>These messages do not indicate an active problem. You can ignore them.</p>

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-6668	<p>When report output is loading and you run another report, the current report is cancelled and new report output is displayed.</p> <p>Workaround: Wait until the report output finishes loading before running another report.</p>
NGS-6634	Storage Group names are limited to contain only ASCII letters, digits and spaces.
NGS-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	The Push History is only shown for subscribers that are online. If a peer is not online, the Push Status field in the Push History will be blank.
NGS-3892	In the ArcSight Command Center, Dashboards that contain a Data Monitor of type 'System Monitor' or 'System Monitor Attribute' will display only the first 100 rows.
NGS-2849	<p>If the refresh rate is set to a low interval so that the refresh happens too frequently, under slow network connections or when having network problems, this might impact browser performance and dashboard behavior.</p> <p>Workaround: To avoid this problem, set the refresh rate to a higher value. You can manually refresh the dashboard if needed.</p>
NGS-2301	<p>While the Dashboards you create in the ArcSight Console can have 3D bar charts, ArcSight Command Center does not support 3D bar charts.</p> <p>Workaround: To see 3D bar charts correctly, you need view them in the ArcSight Console.</p>
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, & 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, & 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"> - An External ID, or - a resource ID, or - a URI
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"> 1. Make sure there are no files in the connector's "current" folder open. 2. Start the connector by using Start > Programs > Connector Programs. Do not start the connectors using the "arcsight agents" command.

General

Issue	Description
NGS-8727	<p>In the Administrator's Guide, in the section "Configuration Changes Related to FIPS," under "Some Often-Used SSL-Related Procedures" > "Generating a Key Pair in a Component's NSS DB," a Note under "On the Console" says, "CN is the External ID of the user you created when running the Manager's setup."</p> <p>It should say, "CN is the IP address or fully-qualified domain name of the Manager you specified when running the Manager's setup."</p>
NGS-8682	<p>In some instances, when an ActiveList is modified at a high rate, the ActiveList cache can become inconsistent with the underlying database table, with the table row count exceeding the configured list capacity. As a result of this inconsistency, updates to entries not found in the cache are sent to the DB as INSERT operations, resulting in a CONSTRAINT VIOLATION exception due to the entry being present in the DB table. In addition, multiple ActiveList tables are updated in the same DB transaction, causing the exception in one ActiveList to roll back updates that had previously been made in other ActiveLists.</p>

Installation and Upgrade

Issue	Description
NGS-8338	If you have customised the file /opt/arcsight/logger/data/mysql/my.cnf, then before you upgrade, make a backup copy of it. The upgrade overwrites this file. After the upgrade restore your customizations from the backed up version of the file.
NGS-7497	<p>Console installation on localized path is working in some Windows 7 machines when installed in a French name like "C:\d'enqu&#xEA;te" but not in other Windows 7 machines.</p> <p>Workaround: Due to the inconsistent behavior in Windows 7 machines, use English filenames only in installation paths. French names in path may cause installation to fail in certain Windows 7 environments.</p>
NGS-7274	<p>In this release, the generation of audit events for the Top Value Counts data monitor is disabled by default. This was enabled in a previous release (ESM 6.0c). If you upgraded to this release, you will not see those audit events.</p> <p>Workaround: If you want to continue seeing audit events for the Top Value Counts data monitor, log in to the ArcSight Console. Edit the Top Value Counts data monitor and select the Send Audit Events option.</p>
NGS-6996	There might be some data monitors disabled after the upgrade, while they are enabled in a fresh installation and vice versa.
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: "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-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.

Issue	Description
NGS-3814	<p>If you reboot your system immediately after the First Boot Wizard completes, but before you run the <code>setup_services.sh</code> command as the "root" user, the machine may come back in an unstable state. Running the <code>setup_services.sh</code> command now may not be able to bring up all Arcsight services.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Do not reboot without running the <code>setup_services.sh</code> command while logged in as the "root" user. 2. If you reboot without running the <code>setup_services.sh</code> command, uninstall and then re-install the product.
NGS-3808	<p>After you select "Next" on the "About to Configure ESM v6.5c" panel, if there is any failure, you will need to uninstall the product before you can reinstall it. Refer to the "Uninstalling ESM" section in ESM Installation and Configuration Guide.</p>
NGS-3445	<p>In some situations, the Installer panel may indicate that the installation was successful even though Web Server fails to start. Refer to the Administrator's Guide on how to manually configure and start the Web Server.</p>
NGS-3344	<p>This release supports ESM installation while logged in as user "arcsight" only.</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>

Pattern Discovery

Issue	Description
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>

