

Release Notes ArcSight ESM™

Version 6.0c

October 11, 2012



Release Notes
ArcSight ESM™,
Version 6.0c

Copyright © 2012 ArcSight, Inc. All rights reserved.

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>

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

This document is confidential.

Revision History

Date	Product Version	Description
10/11/2012	ArcSight ESM Version 6.0c	Release Notes for ArcSight ESM Version 6.0c

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

ESM™ 6.0c Release Notes	1
Welcome to ESM™ 6.0c	1
What's New in This Release	1
CORR-Engine Storage and Archive Management	1
Management Console Interface	1
Resource Migration	2
Upgrade Support	2
Migrating Resources	2
Geographical Information Update	3
Vulnerability Updates	3
Supported Platforms	3
Verifying Secure Delivery	3
Usage Notes	4
Forwarding Connector	4
Domains	4
System Content Active List	4
Browser Support in FIPS with Suite B Mode	4
Starting and Stopping Components	5
Dashboard Warnings	5
ArcSight Web and Management Console	5
Dashboards Containing Geographic Event Graph or Event Graph Data Monitors	5
Online Help in Internet Explorer with Chrome Frame Plugin	5
Performance Considerations When Using Pattern Discovery	6
Deploying a New License	6
Frequently Asked Questions about ESM with CORR-Engine	6
Fixed Issues in ESM 6.0c	9
Analytics	9
ArcSight Console	9
ArcSight Manager	9
Management Console	9
Open Issues in ESM 6.0c	10
Analytics	10
ArcSight Console	12
ArcSight Manager	15

ArcSight Web	17
CORR-Engine	17
Connectors	18
Installation and Upgrade	19
Localization	20
Management Console	20
Pattern Discovery	22

ESM™ 6.0c Release Notes

Welcome to ESM™ 6.0c

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 this release.

CORR-Engine Storage and Archive Management



ESM 6.0c introduces the Correlation Optimized Retention and Retrieval Engine (CORR-Engine), a proprietary data storage and retrieval framework that replaces Oracle. CORR-Engine is optimized to run on systems with a large number of cores and:

- Provides significant performance improvements over Oracle storage
- Reduces storage size significantly for online and archived data
- Receives and processes events at high rates, and performs high-speed searches
- Provides streamlined archive compression, storage, and management

Refer to the Management Console User's Guide for details.

Management Console Interface

ESM 6.0c's new Management Console is a streamlined interface for:

- Monitoring and investigating events using dashboards and drill-downs
- Managing users, storage, and event data
- Accessing information on archives
- Updating licenses and setting up storage notifications



The Management Console is based on Web 2.0 technologies and uses an HTML5 charting engine.

Refer to the Management Console User's Guide for details.

Resource Migration



ESM 6.0c supports the migration of customer-created resources from Oracle storage to the CORR-Engine with a simple engagement from HP ArcSight Professional Services.

Upgrade Support

Instead of an in-place upgrade of Oracle-based ESM, CORRE-based ESM requires a fresh installation. Your HP representatives have a special tool developed for migrating resources from Oracle-based ESM to CORRE-based ESM. The tool needs to be run at the time of installing CORRE-based ESM. Please contact your HP Account Representative for help with this resource migration.

Migrating Resources

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

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

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

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is **GeoIP-532_20120201**.

Vulnerability Updates

This release includes recent vulnerability mappings (August 2012 Context Update) for these devices:

- Snort / Sourcefire SEU 680 updated Faultline, Bugtraq, CVE, Nessus
- Enterasys Dragon IDS updated CVE
- Cisco Secure IDS S661 updated Bugtraq, CVE
- Juniper / Netscreen IDP update 2172 updated Faultline, CVE, MSSB
- TippingPoint UnityOne DV8360 updated Faultline, Bugtraq, CVE, Nessus, MSSB
- Symantec Endpoint Protection updated Faultline, Bugtraq, CVE
- McAfee HIPS 7.0 updated CVE
- Radware DefensePro updated CVE

Supported Platforms

ESM 6.0c is supported on Red Hat Enterprise Linux 6.2 64-bit platform. Refer to the Product Lifecycle document available on the Protect 724 site for further information on supported platforms and browsers.

ESM Patches

This release includes fixes released with ESM 5.0 SP2 Patch 3. ESM 5.0 SP2 Patch 4 and any future patch fixes including ESM 5.2 Patch 1 are not included in this release of ESM 6.0c.

Verifying Secure Delivery

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

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

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

Usage Notes

Forwarding Connector

Make note of the following for the Forwarding Connector for ESM 6.0c:

- The Forwarding Connector for ESM 6.0c is only supported on Red Hat Enterprise Linux 5.5 64-bit. The uninstallation process and any other commands are only supported on Red Hat Enterprise Linux 5.5 for ESM 6.0c.
- ESM 6.0c does not support upgrading to Forwarding Connector 5.2.5.6403.0 from any previous Forwarding Connector release. If you are installing ESM 6.0c in a hierarchical environment, please install Forwarding Connector 5.2.5.6403.0 directly.
- If you are forwarding events from ESM 5.2, the Forwarding Connector version used must be the one released with the latest ESM version, in this case version 5.2.5.6403.0.
- The correlated Forwarding Connector functionality is not supported for ESM 6.0c.
- The automatic forwarding of base events offered with the Correlated Forwarding Connector feature is not supported for ESM 6.0c. On-demand pulling of events is also not supported.

Domains

The Domains feature is not supported for this release.

System Content Active List

The `/All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time` active list is a partially cached active list. At high EPS, there is a possibility of some performance impact.

To work around this issue:

- 1 Edit `/All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time` to change the "Capacity (x1000)" attribute from 10 to 500.
- 2 Restart the Manager for this change to take effect.

Browser Support in FIPS with Suite B Mode

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

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

Starting and Stopping Components



The commands for starting and stopping components in ESM 6.0c are different than the commands for starting and stopping components that were used in prior releases of ESM with Oracle backend.

Also, in ESM 6.0c, the commands for starting and stopping components should be run as user "arcsight".

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

For help on the supported "arcsight_services" enter the following command while logged in as user "arcsight":

```
/sbin/service arcsight_services -help
```

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

Dashboard Warnings

An open dashboard periodically queries the Manager for new data to update itself. If the dashboard doesn't get a timely response for the request, either because of network latency or slow response from the Manager, the web browser will display the following warning dialog:

`Unresponsive Script - A script on this page might be busy or stopped responding"`

Choose **Yes** to clear the message and stop the dashboard from updating itself. You need to manually reload the browser as needed. If you choose no, the dashboard will continue trying to update itself, and the warning dialog will continue to pop up.

ArcSight Web and Management Console

In Safari only: When accessing ArcSight Web from the Management Console for the very first time, after you accept the Manager's certificate, ArcSight Web opens up in a new tab in the browser instead of opening within the Management Console itself.

Dashboards Containing Geographic Event Graph or Event Graph Data Monitors

On Internet Explorer only: In order to load dashboards that contain a Geographic Event Graph or an Event Graph Data Monitor the Google Chrome Frame plugin is required.

Workaround: Install the plugin manually from <http://www.google.com/chromeframe>.

Online Help in Internet Explorer with Chrome Frame Plugin

On Internet Explorer only: When using the Management Console, if you click the Help link, the online Help does not open.

To work around this issue:

- 1 Refresh the browser page or click the refresh button. The browser prompts you whether to accept the Manager's certificate.
- 2 Click Yes. The browser will display the Help content.

Performance Considerations When Using Pattern Discovery

Using Pattern Discovery can cause performance degradation when discovery is performed over a large number of matching events in a high EPS environment. When using an environment with high EPS, define a filter to limit the events sent for Pattern Discovery processing to be less than 1000 EPS.

Deploying a New License

If you need to swap your expired license for a new valid license, do so by running the `managersetup` utility. Refer to the ESM Administrator's Guide for details on running the `managersetup` utility.

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 6.0c? What platforms are ESM 6.0c supported on?

The ESM Manager and CORR-Engine components come integrated in a suite that is installed on a single machine. Single machine install provides better scalability with localized processing and storage tiers. ESM 6.0c should be installed on a single Red Hat Enterprise Linux 6.2 64-bit machine. The Manager and CORR-Engine cannot be installed on separate machines.

See the section, "[Supported Platforms](#)" on page 3, for information on supported platforms.

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

The ESM 6.0c 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 ArcSight Professional Services for help with the sizing requirements.

What are the hardware requirements for ESM 6.0c?

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

Can ESM 6.0c be part of a mixed hierarchical architecture with ESM 5.x using a Forwarding Connector?

Yes. You can forward events from ESM 5.0 SP2 with latest patch or 5.2 with latest patch to ESM 6.0c. However, we recommend that you do not send events to ESM 5.x, and instead send them directly to ESM 6.0c.

Will existing licenses work?

If you have a valid existing ESM license, you can use it with ESM 6.0c.

Can I continue to use my existing Loggers with ESM 6.0c?

Yes. You can forward events from Logger 5.3 to ESM 6.0c and vice versa.

Can I upgrade my existing ESM installation to ESM 6.0c?

Upgrade of an existing ESM installation is not supported for ESM 6.0c. However, you can migrate your resources from your existing Oracle-backend ESM installation to your ESM 6.0c installation. See [“Migrating Resources” on page 2](#) for further details on this.

How do I get to manage.jsp?

`manage.jsp` and other advanced troubleshooting tools, such as `license.jsp` and `resource.jsp`, are available from the new Management Console by adding the following string to the end of the Management Console home page URL: `?advancedadmin=true`. For example,

`https://servername:8443/www/management-ui/com.arcsight.product.management.ui.WorkbenchLauncher/?advancedadmin=true`

`manage.jsp` and the other advanced troubleshooting tools are not supported for general customer use without guidance from HP ArcSight 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 Management Console User's Guide for further details.

How do I backup and restore my data in ESM 6.0c?

Refer to the ESM Administrator's Guide and the Management Console User's Guide for details on how to backup and restore your data.

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

Once you have installed the ESM 6.0c software, you can migrate your resources from a legacy ESM 5.x installation with the assistance of your HP ArcSight Account Representative.

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

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

What fields are indexed in CORR-Engine?

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

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

Yes. Please contact HP ArcSight 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 Management Console.

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.
- Refer to the section, ["Forwarding Connector" on page 4](#) on forwarding of events, specifically note that auto-forwarding of base events is not supported.
- Daily partitioning on trend and session list data is replaced by weekly partition.

Fixed Issues in ESM 6.0c

The following issues that were reported in the previous ESM release have been fixed in this release of ESM 6.0c.

Analytics

Issue	Description
NGS-448	In some cases, a query would run for more than 10 hours (but less than 20 hours) before being canceled. The system now detects these situations and causes the query to time out.

ArcSight Console

Issue	Description
NGS-2167 TTP#66337	The server.log file showed an exception when a custom view dashboard was launched on a system running in FIPS mode. This has now been fixed; Custom View dashboards on a FIPS mode system are launched in an external browser.
NGS-1795	On non-Windows platforms, when you viewed dashboards with Custom layout option in the Console, you got an error, "Failed to create embedded browser, launching external browser" This issue has now been fixed.

ArcSight Manager

Issue	Description
NGS-1847	InActiveList condition on a multimapped active list did not work when all fields (both key and non-key fields) were not mapped. This did not affect non-multimapped active lists. The workaround was to map all the key and value fields. This was a partial workaround, because all the mapped fields need to match the values stored in the MultiMapAL. This has now been fixed.

Management Console

Issue	Description
NGS-2259 TTP#68477	This release supports using bar charts in a dashboard.
NGS-2258	The issue with a dashboard rendering slowly in the browser has been fixed in this release.
NGS-2256	This release supports using stacked bar chart in a dashboard.
NGS-2245	In the Custom Layout of a dashboard, if you tried to change the display format of a data monitor, say from "Bar Chart" to "Table" and you saved the dashboard, the next time that you reloaded the dashboard, the data monitor would still display in the "Table" format. The display format could not be changed in the Custom Layout. This bug has been fixed.

Issue	Description
NGS-2184	The issue with a dashboard occasionally not loading predefined background color/image has been fixed in this release.
NGS-1523	User group creation was failing when the user group name field contained '&'. The system now detects '&' as an invalid character and does not create the resource until valid characters are used.
NGS-1435	The Pie Chart view of a Data Monitor or Query Viewer used to have a legend area that, if too long, would shrink the pie chart considerably. The pie chart no longer has a legend area.
NGS-1425	The Custom Layout view of a Dashboard, Data Monitor, or Query Viewer displayed in chart view such as bar chart, pie chart or line chart was failing due to an issue with the Adobe Flash Player. The Adobe Flash Player is no longer used.
NGS-1149	When using the Internet Explorer browser to access the Management Console, in the "Dashboards" section of the Management Console, the Close Dashboard menu command appeared enabled even though it was not an applicable command. This issue has now been fixed.
NGS-1072	Displaying EventGraph data monitors from within the ArcSight Console custom layout internal browser is no longer supported. You must launch an external browser from ArcSight Console custom layout or use the Management Console dashboard module in order to view any dashboard with EventGraph data monitors.

Open Issues in ESM 6.0c

These open technical issues merit your review to avoid difficulties.

Analytics

Issue	Description
ESM-49187	The Text (Column Names/Field Names/Aliases) in the Table Header do not display CJK characters even if the table has been set to use Arial Unicode MS font.
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 will be suppressed.
ESM-48307	The DeviceEventclassId for Windows 2008 has the same value as Windows 2003.
ESM-47918	Occasionally, TRM does not return an appropriate response when an update to Quarantine Node by IP command is sent.
ESM-40449 TTP#66622	When exporting events from the Case Details channel, archived events do not get exported.
ESM-39405 TTP#64400	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-38079 TTP#62044	If you rename a resource that has dependent resources, do not re-use the deleted resource's name when creating another resource of the same type because the dependent resources may refer to the new resource with the old name.

Issue	Description				
ESM-37810 TTP#61524	For scheduled reports, when the "Run as" user's read and write privileges are taken away, the scheduled report is generated by the user who created the schedule (and not by the "Run as" user). If the "Run as" user has read privilege only, then the report is not generated.				
ESM-35070 TTP#54507	<p>Verify Rules with Events (replay with rules) does not work for the following types of active lists:</p> <ul style="list-style-type: none"> - An event-based active list with values - A field-based active list with values, where all fields are mapped to event fields <p>Verify Rules with Events does work for other types of active lists. Also, valid active lists work properly with real-time rules when they are deployed, including the two types of active lists described above.</p>				
ESM-34531 TTP#53435	When you set the Schedule Frequency for a report, the Next Run Time field is displayed incorrectly in the Editor. Even though the time is displayed incorrectly, the report runs at the time specified in the editor.				
ESM-29633 TTP#40230	<p>Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (For example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.</p>				
ESM-29348 TTP#39407	The Scheduled Time column in the Scheduled Runs view covers both time ranges for runs that have already occurred and for runs that are pending. As a result, you will see some discrepancy in the time ranges shown in the column. For example, against the runs that have already occurred, you will see the lower end of the time range. (For trends set to run hourly, if the time range is between 1:00 pm - 2:00 pm you will see 1:00 pm). The pending runs show the upper range (if the time range is between 1:00 pm - 2:00 pm you will see 2:00 pm). Trends that have already occurred will have a time difference that reflects the trend query schedule (for example, one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (for example, 24 hours if run once a day).				
NGS-3955	<p>The /All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time active list, is a partially cached active list. At high EPS, it is possible that there could be some performance impact.</p> <p>Workaround: Edit /All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time and change the "Capacity (x1000)" attribute from 10 to 500.</p>				
NGS-3686 TTP#61694	When you try to delete a Trend being used in a Query and in turn used in a Query Viewer, you will get an error and the Trend will not be deleted. This is a dependency chain. Remove the use of this trend in other resources first before using it.				
NGS-3294	Base events cannot be retrieved from the source Manager by the destination Manager.				
NGS-3139	<p>While trying to query on a Case, please specify the ID of the user instead of the name of the user.</p> <p>For instance,</p> <table> <tr> <td>owner=admin</td><td>--- won't work</td></tr> <tr> <td>owner=1UOtZMTkBABCA0qd7zsU1IQ==</td><td>--- will work</td></tr> </table>	owner=admin	--- won't work	owner=1UOtZMTkBABCA0qd7zsU1IQ==	--- will work
owner=admin	--- won't work				
owner=1UOtZMTkBABCA0qd7zsU1IQ==	--- will work				

Issue	Description
NGS-2917	<p>When a lightweight rule is scheduled, the rule actions that update data lists may not work correctly if the fields mapped to the list columns are not used in any rule conditions.</p> <p>Workaround: Add a simple condition on the mapped fields. For example, if field DeviceCustomNumber1 is used in the mapping for an AddToList action, add a rule condition such as "DeviceCustomNumber1 IS NOT NULL". Then, the field value for that event will be queried from the database when the scheduled rule task is executed.</p>

ArcSight Console

Issue	Description
ESM-47213	<p>Case-related events are copied to a special table so they can remain available after being archived. The channel is unable to find and display such events correctly after the partition is archived.</p> <p>Workaround: Use the case event editor or Reports, which can correctly find and display these events.</p>
ESM-41641 TTP#69565	<p>On Macintosh only: If you open a channel, select some rows, right-click on them and select Print Selected Rows from the resulting menu, it causes the Console to crash.</p> <p>Workaround: Before you start the Console, make sure to set up a default printer to which to print. This problem occurs when you do not have a printer set up.</p>
ESM-41019 TTP#67856	<p>When you have client-side authentication set up, if the Manager is configured with the "Password Based and SSL Client Based Authentication", you will get an error when accessing the ESM documentation using both the embedded browser in the Console as well as the external browser.</p> <p>Workaround: Generate a key pair for the browsers and import the browser's certificate into the Manager's truststore. Alternatively, copy the Console's key into the browser's keystore. See the ESM Administrator's Guide for details on how to do this.</p>
ESM-40587 TTP#66906	<p>Correlation events may occur before the base event that triggered the correlation event in channels sorted by time. This happens if the event end time for the correlation event is the same as that for the base event.</p> <p>Workaround: Add a sort column in the channel to sort events, first by end time, and second by type of event. Base event type is 0 and correlation event type is 1.</p>
ESM-39980 TTP#65708	<p>The Console can become unresponsive if you access other resources while building category models with a large number of actors.</p>
ESM-39963 TTP#65671	<p>If an Active Channel uses a filter that applies conditions to a List data type field, then multiple rows will be seen in the Active Channel for the same event or resource.</p> <p>Ignore the duplicate rows.</p>
ESM-39856 TTP#65477	<p>If you use the embedded browser in Windows to view a report, the report may not appear until you resize the panel.</p> <p>Workaround: Resize the panel before running a report. You may want to try several resizings to get the desired results.</p>
ESM-39829 TTP#65421	<p>Deleting actors will require category models, if any, to be re-built. Each rebuild may take seconds. So, when thousands of actors are deleted, the whole deletion period may last for hours since actor deletion launches a category model rebuild.</p>

Issue	Description
ESM-39331 TTP#64251	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 the Actor channel uses instead of adding them directly to the channel.
ESM-38961 TTP#63568	In the Image View mode, when a background file is uploaded, the Console does not provide an option for a location. The file automatically gets uploaded into your personal folder. Workaround: After the upload, move the file to a preferred folder.
ESM-37344 TTP#60500	On the Manager, when a large number of cases reside in a single group, you can't pick a case for "Add to Existing Case" rule action in the Rule editor. This is because the resource selector only shows leaf nodes when there are less than 1000 cases in a group. This happens for all resources. Workaround: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.
ESM-36055 TTP#57050	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, you will not get an error saying that you are not able to view some resources in the query due to lack of sufficient permissions.
ESM-35998 TTP#56865	On Linux only: If you right-click on the port field in a channel and select Integration Commands > Portinfo (Linux), you will get an error.
ESM-33453 TTP#51094	On Unix systems: The drag-and-drop feature does not work on the Console. Workaround: Use the cut-and-paste feature instead.
ESM-33440 TTP#51072	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-33360 TTP#50968	If you delete an escalation-level notification resource, you will receive the error, "Group does not exist" in the console.log file. This error is incorrect and can be ignored.
ESM-32705 TTP#49608	In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range. Workaround: Delete the existing color mapping and create a new one with the color mapping of your choice.
ESM-28890 TTP#38270	While installing a package, if you cancel the installation before it is completed, the Import button is disabled. Workaround: Refresh the Console or log in to the Console again to enable this button.
ESM-27970 TTP#36148	To search for Resource IDs that begin with non-alphanumeric characters (such as the Resource IDs for Trends and Queries), enclose the ID in double quotes. For example, to search for <code>^VVsOXg4BABCAIEuBhILMyg==</code> Enter <code>"^VVsOXg4BABCAIEuBhILMyg=="</code> in the query text field.

Issue	Description
ESM-26488 TTP#33835	<p>If you import the content of an older package into an existing newer package, the contents from the two packages get merged. The resulting package will consist of contents from both packages. The relationships will be merged, but the attributes will be picked up from the old package.</p> <p>Workaround: Export the new package to a bundle file so that you can recover it if need be. Then delete the new package before you import the old one.</p>
NGS-3930	Adding a stacked bar chart to a dashboard where this chart is based on a Query Viewer on an Active List can cause the Console to hang.
NGS-3850	If you have trouble with the internal browser on a Win64 system, please use the external browser.
NGS-2499	<p>The time field in the Image Dashboard will be displayed as a number instead of displaying as formatted date and time.</p> <p>Workaround: Use regular dashboard instead of Image Dashboard.</p>
NGS-2241	<p>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. To fix this, you must define the arrangement and save it. This can be done in one of these ways:</p> <ol style="list-style-type: none"> 1) Using auto-arrange: Go to Edit->Auto Arrange and then click 'Save' to preserve the changes. 2) Manual arranging: Go to Edit->Arrange and move/resize all dashboard elements to the desired position. When finished, click 'Done Arranging' and then 'Save'.
NGS-1262	If a dashboard contains a Query Viewer that has a large row limit, the Console may hang while loading this dashboard in Custom Layout view. It is a good practice to keep the row limit of Query Viewers to less than 100 before viewing the dashboard in custom layout format.
NGS-1088	<p>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.</p> <p>Workaround: Avoid using Event Annotation Flag in filter conditions.</p>
NGS-146	<p>Occasionally, event-based Active Channels that include InCase filtering condition will not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit.</p> <p>This issue will rarely be seen because the CORR-Engine provides powerful event compression and it can support very long retention periods given sufficient disk space. This reduces the chance of events expiring while bound to an open case.</p>

ArcSight Manager

Issue	Description
ESM-41331 TTP#68451	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: To produce a correct report, run the resource validation script manually using '-persist false' as a parameter:</p> <pre>arcsight resvalidate -persist false</pre> <p>In general, if you need to run the resource validation script, you have to run it twice: the first time with '-persist true' (default) to validate and fix invalid resources, and the second time with '-persist false' to generate a correct report:</p> <pre>arcsight resvalidate arcsight resvalidate -persist false</pre>
ESM-40889 TTP#67567	<p>The "group: 101" audit event may fail to be sent in some cases where there are many role memberships being added or changed for an actor. There will be an error in the server log related to this, which includes the IDs of the affected objects.</p>
ESM-37488 TTP#60808	<p>When you export a large Active List with 10 million entries or more, or export rules that use such Active Lists, you will see an exception in the server.std.log file. Additionally, the Manager runs out of memory and therefore 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-33462 TTP#51112	<p>Stages resources are editable from the ESM Console, although these should not be moved or customized. (See ESM Console Navigator > Stages resource tree.) Keep stages provided as standard content in the given folders and do not move them into another folder. Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created. (For more information, See the "Standard Content" topic in the Console Help.</p>
ESM-31433 TTP#46276	<p>You may see the following exception in the Manager's log file:</p> <pre>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</pre> <p>Workaround: This error automatically gets resolved within one week of the Manager startup during which time the Manager rebuilds the resource search index (done weekly). Optionally, you can manually do a rebuild at any time by running this command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create -m <manager-hostname> -u <admin-user-name> -p <password></pre>
ESM-30670 TTP#43678	<p>If the search index file becomes corrupted, the search index will be out-of-date and the following message appears in the Manager's log file:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Re-generate the index by issuing the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create</pre>
ESM-30314 TTP#42730	<p>You cannot move an asset using Auto Zone if the asset is locked.</p>

Issue	Description
NGS-3909	If you have a high-end system (refer to specifications given in the System Requirements section of the ESM Installation and Configuration Guide) that's running content that requires a high level of system resources, and/or high EPS, contact HP ArcSight Customer Support for instructions on how to increase the heap size beyond 16 GB if needed.
NGS-3856	<p>When you try to display an Active List with a large number of entries (for example 10 million entries), you will see an error in the server.log file.</p> <p>Workaround: Increase the memory size for ESM to ensure that the Active List size is within limit. Also, if possible avoid displaying Active Lists with large number of records.</p>
NGS-3825	If the field size of an event exceeds 32 KB, that event does not get persisted.
NGS-3803	The command "arcsight manager-reload-config" fails to dynamically reload the configuration. Restart the Manager if you make any configuration changes such as the ones that go in the config/server.properties file.
NGS-1937 TTP#56123	<p>The Archive tool can occasionally fail to import entries into an active list due to transient errors. In such situations, you may not see any errors, but the list does not get populated.</p> <p>Workaround: Re-import the same package.</p>
NGS-1718	If an event-based active list contains both a resource reference (for example, Agent Zone) and a related field (for example, Agent Zone Name), then when adding a new active list entry in the Console editor (for example, using the "+" button in the Show Entries display), care should be taken that the related field value matches the value implicit in the resource itself. In the example given, the Zone Name should match the Name of the Zone resource. This can cause some cases of active list lookup (for example, trying to "Edit Entry" in the Show Entries pane), not to match. In this case, it will result in an unpopulated edit pane.
NGS-1449	When you shut down services using the arcsight_services command, you may see exceptions in the log file. These exceptions are due to timing issues of different components and can be ignored.
NGS-264	When integration with iDefense is enabled and you create a Case in ESM, the Case notes may have some special characters garbled. The text can alternately be viewed in iDefense or in the Event Inspector panel.
NGS-172	<p>Base events do not get annotated automatically after rules trigger.</p> <p>Workaround: Annotate the events manually.</p>

ArcSight Web

Issue	Description
ESM-41321 TTP#68431	If the report name contains the hash character "#", there may be a problem displaying the report correctly. In such a case, remove the "#" character from the report name.
ESM-35801 TTP#56258	If you create a Case and set the Estimated Resource Time in ArcSight Web, it does not get set. Workaround: Define this setting on the Console. See the Console online Help for steps to do this.
ESM-33922 TTP#52336	On ArcSight Web, there is no row limit imposed on Query Viewer chart displays (unlike on the ESM Console). Query Viewer charts with more than 100 rows do not display properly and are virtually unreadable. On the ArcSight Console, the chart renders only the first 100 rows and displays an error message indicating that only 100 rows can be properly displayed. No such restriction is available for Query Viewer charts on ArcSight Web dashboards, so rows beyond the 100th row will not display properly on the Web. Workaround: In the Console, set row limits on Query Viewers. This will control chart displays in the Console and ArcSight Web. Determine which Query Viewers you want to display as charts. In the ArcSight Console, edit those Query Viewers to set the Row Limit to 100 (or less). To do this: 1. Log in to the ArcSight Console. 2. Select Query Viewers in the Navigator. 3. Right-click the Query Viewer you want to edit. 4. In the Query Viewer Editor, if Use Default is enabled, click to deselect it. 5. Enter a row limit of 100 or less. 6. Click Apply or OK to save the changes.
ESM-30675 TTP#43702	Due to a limitation in Adobe Flash Player, to view dashboards within ArcSight Web on a 64-bit operating system, you must use a 32-bit browser with a 32-bit version of Flash player installed. Refer to the Adobe web site that discusses this issue: http://www.adobe.com/go/6b3af6c9
NGS-3605	The Management Console does not support a user-configurable banner which is commonly used to display custom login messages.
NGS-2017	The "arcsight webserversetup" wizard does not detect the certificate name of the webserver. It defaults to displaying the hostname or IP address depending upon the OS configuration. If you run this wizard, make sure to change the webserver name to the name as it appears on the certificate of the Manager or the webserver.

CORR-Engine

Issue	Description
NGS-3948	When restoring archives from an old ESM 6.0c system to another ESM 6.0c system, if the archives contain forwarded events, the restore of that archive will fail due to a highly restrictive eventID check.

Issue	Description
NGS-3689	<p>If MySQL needs to be restarted, we recommend using the following steps:</p> <ol style="list-style-type: none"> 1. Stop the Manager by running: <code>/sbin/service arcsight_services stop manager</code> <p>This is because the Manager communicates with MySQL. If the Manager is running, MySQL takes longer to close the TCP communication, causing more error messages to be logged in the log files.</p> <ol style="list-style-type: none"> 2. Stop MySQL by running: <code>/sbin/service arcsight_services stop mysqld</code> 3. Start MySQL by running: <code>/sbin/service arcsight_services start mysqld</code> 4. Start the Manager by running: <code>/sbin/service arcsight_services start manager</code>
NGS-1429	You can only restore archives from a single CORR-Engine. Do not combine archives residing in multiple CORR-Engines.

Connectors

Issue	Description
NGS-3806	<p>Auto-import of the Manager's certificate does not work if your connector is installed in FIPS with Suite B mode.</p> <p>Workaround: Import the Manager's certificate manually. Refer to the ESM Installation and 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 Windows machines, while a connector is being upgraded from the ArcSight Console, if any process is using the connector's 'current' folder, the upgrade fails.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Make sure that you don't have any files in the connector's 'current' folder open. 2. Do not start the connectors using the 'arcsight agents' command. Instead, start the connector from <code><Start> -> <Programs> -> <Connector Programs></code>

Installation and Upgrade

Issue	Description
NGS-3971	<p>When running the installer in console mode, make sure that a X11 (X Window) is NOT configured for the console. An X11 setup will cause the installation to abort with the following exception in the database.configuration.log file:</p> <pre>"java.lang.NoClassDefFoundError: Could not initialize class sun.awt.X11GraphicsEnvironment".</pre> <p>Should this happen, follow the clean-up instructions in the ESM Installation and Configuration Guide and re-launch the installer from a console that does not use X11 (X Window).</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-3926	<p>When uninstalling ESM 6.0c with migrated resources (after running the Resource Migration tool), to ensure that all files get removed under the /opt/arc sight/ directory, uninstall the Resource Migration tool first. Uninstalling the Resource Migration tool before uninstalling ESM 6.0c will allow for clean uninstallation of ESM 6.0c.</p>
NGS-3880	<p>If /opt/arc sight/ has been created as a separate file system, directories other than those installed by ESM 6.0c may exist. These directories should not be deleted. The following directories under /opt/arc sight/, when removed, will uninstall ESM 6.0c:</p> <ul style="list-style-type: none"> logger manager services suite web
NGS-3871	<p>Under certain circumstances, the Uninstaller may not be able to remove all ESM 6.0c files under the /opt/arc sight/ directory. Refer to the Troubleshooting appendix in the ESM Installation and Configuration Guide on how to do the cleanup manually.</p>
NGS-3839	<p>Occasionally, the First Boot Wizard may fail to proceed due to some errors. If this happens, you will need to terminate the process. After checking the logs and correcting the errors, follow the clean up instruction in the ESM Installation and Configuration Guide and re-launch the installer.</p>
NGS-3814	<p>If you reboot your system immediately after the First Boot Wizard completes, but before you run the setup_services.sh command as the "root" user, the machine may come back in an unstable state. Running the setup_services.sh command now may not be able to bring up all arc sight services.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Do not reboot without running the setup_servives.sh command while logged in as the "root" user. 2. If you reboot without running the setup_services.sh command, uninstall, then re-install the product.

Issue	Description
NGS-3808	After you hit "Next" on the "About to Configure ESM v6.0c" panel, if there is any failure, you will need to uninstall the product before you can reinstall it. Please follow the "Uninstalling ESM" section in ESM Installation and Configuration Guide.
NGS-3445	In some situations, the Installer panel may indicate the installation is successful while Web Server fails to start. Refer to the ESM Administrator's Guide on how to manually configure and start the Web Server.
NGS-3344	This release supports ESM installation while logged in as user "arcsight" only.
NGS-3322	Due to the timing of some components' start-up, there may be some harmless error messages in the log files such as: [FATAL][default.com.arcsight.logger.distributed.DirectConnection\$ReadChannel][run] java.io.IOException: end of communication channel [FATAL][default.com.arcsight.logger.distributed.ClientDirectConnection][run] java.nio.channels.ClosedChannelException
NGS-3067	When configuring the product using the First Boot Wizard, if you use a wrong IP address or an unresolved IP address in the Manager Hostname panel, the First Boot Wizard will continue installing but fail during Arcsight Web configuration. Make sure the Manager's hostname or IP address is correct and can be resolved otherwise the Manager will not start.

Localization

Issue	Description
NGS-3824	Some pages and labels have not been translated into the localized language, so they will appear in English.
NGS-2435	For non-English locale environments, only English characters are supported for user name and password. Using non-English characters for user name and password might result in authentication issues.

Management Console

Issue	Description
NGS-3892	In the Management Console, Dashboards that contain a Data Monitor of type 'System Monitor' or 'System Monitor Attribute' will display only the first 100 rows.
NGS-3862	In the Management Console, under Administration->Configuration Management->Server Management the Save button does not get enabled right away after changing the value of a field, but only after the field that is being changed loses the focus. Workaround: If you make a valid change, click the Save button even if it is grayed out.
NGS-3858	The minimum and default heap size for the Manager is 8GB, the maximum heap size is 16GB. You can change this size based on total available memory on your system. The error message related to this heap size in the Management Console does not reflect this accurately. If you need to configure the heap size beyond 16 GB, please contact HP ArcSight Customer Support before doing so.
NGS-3084	Global variable fields do not get displayed in an Image Dashboard.

Issue	Description
NGS-3001	<p>On some Macintosh platforms, when running FireFox 3.6.x, you will not be able to open the right-click menu for Image Dashboards of graph/chart type.</p> <p>Workaround: You can use the Safari browser and use the right-click menu for image dashboards of graph/chart type.</p>
NGS-2849	<p>If the refresh rate is set to a low interval so that the refresh happens too frequently, under slow network connections or when having network problems, this might impact browser performance and dashboard behavior. To avoid this problem, set the refresh rate to a higher value. You can manually refresh the dashboard if needed.</p>
NGS-2301	<p>The Management Console does not support 3D bar charts.</p>
NGS-1582	<p>In the 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 happen if you have created some customCells using the ESM Console. If you see such a folder, do not change the ACL settings on it. Doing so will affect the working of custom cells in ESM 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. It is a good practice to keep the row limit of Query Viewers below 100 before viewing the dashboard in custom layout format.</p>
NGS-1283	<p>You must have administrator privileges to access the user/connector management feature.</p>
NGS-1275	<p>The Notification Groups attribute is missing from the connector management page.</p> <p>Workaround: Use the ESM Console to view the Notification Groups through the Configure Connector option.</p>
NGS-1256	<p>In the Management Console, after clicking the tab to navigate into a module, you may encounter a blank screen.</p> <p>Workaround: Refresh the screen by reloading the browser page.</p>
NGS-1254	<p>When using some versions of the Firefox browser, occasionally your login fails and you see the following exception in the server.log file:</p> <p>" java.lang.SecurityException: Blocked request without GWT permutation header (XSRF attack?)"</p> <p>This happens because of an issue in Firefox which occasionally drops GWT headers beginning with x.</p> <p>Workaround: Add the following property to the server.properties file:</p> <p>cross.domain.enabled=true</p> <p>and restart the Manager in order for it to take effect.</p>
NGS-277	<p>You cannot select the docked items (icons such as admin, dashboards etc.) using the keyboard shortcuts. The only way to select them is by using the mouse.</p>

Pattern Discovery

Issue	Description
ESM-35048 TTP#54452	A java.lang.InterruptedException might be logged in the ESM Manager server.std.out.logs file when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.
NGS-3527	Pattern Discovery jobs can be resource intensive. Under high EPS, Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. We recommend that you reduce the number of events over which the Pattern Discovery search runs and/or frequency of Pattern Discovery jobs when running a system with high EPS.