

Release Notes

ArcSight ESM 5.5

August 29, 2013



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

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

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

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

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

Contact Information

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.arcsight.com

Revision History

Date	Product Version	Description
08/29/2013	ESM 5.5	Release Notes for ESM 5.5 release

Contents

ArcSight ESM Version 5.5	5
Welcome to ArcSight ESM Version 5.5	5
What's New in This Release	5
Rules	5
Debug Event Priority Rating	5
Lists	5
Reports	6
Variable Functions	6
Oracle Support	6
Oracle PSU	6
Upgrade Support	6
Geographical Information Update	7
Vulnerability Updates	7
Forwarding Connector	7
Usage Notes	7
ArcSight Web's Browser Support	7
Oracle Password Expiration Issue	7
Session Expiration in ArcSight Web	8
Browsers and Custom View Dashboards	8
JRE on Macintosh	8
Fixed Issues in 5.5	9
Analytics	9
ArcSight Console	9
ArcSight Database	10
ArcSight Manager	10
ArcSight Web	11
Installation and Upgrade	11
Open Issues in 5.5	11
Analytics	11
ArcSight Console	14
ArcSight Database	17
ArcSight Manager	18
ArcSight Web	20
Installation and Upgrade	21

Pattern Discovery	23
-------------------------	----

ArcSight ESM Version 5.5

Welcome to ArcSight ESM Version 5.5

ArcSight Enterprise Security Management (ESM) 5.5 improves the feature set for its security and event management platform and its identity correlation functionality.

What's New in This Release

This section contains a summary of the improvements and new capabilities introduced as part of the ArcSight ESM 5.5 release.

Rules

- Pre-persistence rule type

A third rule type, pre-persistence, is now available. This rule type uses the Set Event Field action to modify base events before they are enriched and persisted to the database, unlike other rule types that set fields on rule correlation events. Event fields are modified every time an incoming event matches the condition specified for the rule. The rule does not have to wait to go through the correlation enrichment process before executing the action. Event fields set by a pre-persistence rule are available to normal, real-time rules that run during the normal correlation process.

- Rule action to update a case stage

The rule actions Create a New Case and Add to Case now include a new field to set the case's stage.

Refer to Chapter 12, "Rules Authoring," in the ArcSight Console User Guide, for information about rules.

Debug Event Priority Rating

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

Refer to the topic "Priority Calculations and Ratings," in the "Reference Guide" section of the ArcSight Console User Guide for more information about the Priority formula that calculates priority scores.

Lists

You can now specify active and session lists to be case-sensitive or case-insensitive. You can further refine the case insensitivity setting for key fields only, value fields only, or both.

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

Reports

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

Variable Functions

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

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

Refer to the topic “Variable Functions,” in the “Reference Guide” section of the ArcSight Console User Guide for information about variables and functions.

Oracle Support

ESM 5.5 uses Oracle 11.2.0.3. If you are using Oracle 11.2.0.2, you can upgrade to Oracle 11.2.0.3 after upgrading the ArcSight Database component. In the Upgrade Guide, see the chapter “Upgrading Oracle Database,” for details on how to upgrade Oracle. We strongly recommend that you upgrade to Oracle 11.2.0.3.

If you are using Oracle 11.2.0.1 on Windows, you must first upgrade your Oracle software to 11.2.0.2 by upgrading to ESM 5.0 SP2 Patch 2 or Patch 3 before upgrading to 5.5. Refer to the release notes for the target ESM version for detailed instructions on upgrading to it.

Oracle PSU

Refer to the latest ArcSight Oracle Patch Set Update (PSU) Release Notes for Oracle Patch Set Update (PSU) and OPatch information.

Upgrade Support

ESM 5.5 is only supported on 64-bit Windows and Linux. The following upgrade paths are supported for this release:

- ESM 5.0 SP2 Patch 4 (or greater) to ESM 5.5
- ESM 5.2 Patch 2 (or greater) to ESM 5.5

Please refer to the upgrade guide for more information on upgrade instructions. If you are on a 32-bit operating system, please contact HP ArcSight Customer Support for information on migrating your Oracle to a 64-bit system.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20130201.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU 856	Faultline, Bugtraq, CVE, Nessus
Enterasys Dragon IDS	CVE
Cisco Secure IDS S707	Bugtraq, CVE
Juniper / Netscreen IDP 2252	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
TippingPoint UnityOne DV8431	Bugtraq, CVE
ISS SiteProtector	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, Nessus, MSSB
McAfee HIPS 7.0	CVE
Radware DefensePro	CVE

Forwarding Connector

This release comes with Forwarding Connector version 5.1.7.6151 for 64-bit systems.

Usage Notes

Please review the following points to ensure smooth operation.

ArcSight Web's Browser Support

ArcSight Web does not work with Microsoft's Internet Explorer 10. Use an earlier version of IE with ArcSight Web.

Oracle Password Expiration Issue

Starting with 11g, by default, Oracle has set the passwords to expire 180 days after the account has been created. This causes connectivity issues to the database after the 180 day default period on both new installs as well as on upgraded systems. This was not the case with Oracle 10g.

If you run into this problem of expired password, then do the following to set the password to never expire.

- 1 % arcdbutil sql
- 2 Enter user-name: / as sysdba

- 3 SQL> select PROFILE from dba_users where username =
'<arcsight_schema_owner>';
- 4 SQL> alter PROFILE <profile result from step 3> limit
PASSWORD_LIFE_TIME UNLIMITED;
- 5 SQL> exit;

In 11g, by default, Oracle has set the failed login attempts value to 10. If the account gets locked for exceeding the number of failed login attempts, use the following to resolve the issue.

- 1 % arcdbutil sql
- 2 Enter user-name: / as sysdba
- 3 SQL> alter user <arcsight_schema_owner> account unlock;
- 4 SQL> exit;

For more information on changing this behavior, refer to the Knowledge Centered Support (KCS) article KM1273029, which is available from the HP SSO portal at <http://support.openview.hp.com/selfsolve/document/KM1273029>

Session Expiration in ArcSight Web

When an ArcSight Web session expires, the URL changes and you see a login screen that expects you to enter a user ID and a password. If you are using SSL authentication, CAC, or RADIUS authentication which do not use a username/password combination to authenticate, relaunch ArcSight Web and change the URL back to `https://<servername>:9443/arcsight/web`. For SSL, a certificate is used to login. For CAC or Radius authentication a dialog opens prompting you to enter a pin or passcode.

Browsers and Custom View Dashboards

With dashboards in custom view mode, the dashboard may not launch or charts are not displayed. This is because the Adobe Flash Player is required and you are either using the embedded browser or the 64-bit external browser. If you are using a 64-bit browser, change that to 32-bit in your Console's Preferences menu and then download Adobe Flash Player.

If you are using an embedded browser, download Mozilla Firefox 2 or 3, then restart the Console. The embedded browser copies the Adobe Flash Player from Firefox. You need not change any Preference settings in this case. You may continue to use Internet Explorer and uninstall Firefox if desired.

Refer to the following site for more information about the Adobe Flash Player plug-in and 32-bit browsers:

<http://kb2.adobe.com/cps/000/6b3af6c9.html>

JRE on Macintosh

On the Macintosh 10.7 platform, install JRE 1.6.0_43 before installing ESM 5.5.

Fixed Issues in 5.5

Analytics

Issue	Description
ESM-50636	<p>The /All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time was a partially-cached active list. At high EPS, it sometimes created a performance impact.</p> <p>The list has been changed from a partially-cached active list to a regular active list and the capacity is changed to 500k, so this issue no longer occurs.</p>
ESM-49745	There was NullPointerException when scheduled rule was executed. This issue is resolved.
ESM-38079	<p>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.</p> <p>This behavior is now documented in the ArcSight Console User's Guide.</p>

ArcSight Console

Issue	Description
ESM-50907	<p>Previously the HTML text in a payload viewer used non-HTML line breaks.</p> <p>These are now replaced with HTML line breaks: <code>
</code>.</p>
ESM-50539	To avoid confusion, Millisecond(s) has been added to the timeout label to identify how long the dialog will display before timing out and closing.
ESM-50538	With this ESM 5.5, the Add/Remove/Replace column selector has been reverted back to the same look as previous ESM versions, such as in ESM 5.0 SP2 P3, such that it moves the root level columns back into a "root" group.
ESM-50407	<p>When you select Help > About in the ArcSight Console, the link to ThirdParty_Copyright_Notices_and_License_Term.pdf did not work.</p> <p>It now works.</p>
ESM-49187	<p>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.</p> <p>The workaround is to manually apply the font (Arial Unicode MS) for each header cell in the template designer.</p>
ESM-33943	<p>Previously, if you moved a resource and then ran a resource search, the search result would output the wrong URI as the original location, even if you wait for next Resource Search Index Updater. However, the detailed information in the result was correct.</p> <p>Now the URI is correct.</p>
ESM-33489	When connector was updated or the Manager restarted, sometimes it showed incorrect user's name in the editor. Now, when it is changed by a user, it shows the correct username. If the Manager is restarted, then it shows a blank username.

ArcSight Database

Issue	Description
ESM-50416	<p>On versions before ESM 5.5, audit was enabled by default and caused the audit table to grow.</p> <p>On a fresh ESM 5.5 install, the audit is disabled by default. For an upgraded system, use the following dictionary table to identify whether the create session audit is enabled.</p> <pre>select * from DBA_PRIV_AUDIT_OPTS;</pre> <p>To verify that the audit table is not growing, first truncate the sys.aud\$ table:</p> <pre>truncate table sys.aud\$</pre> <p>Then...</p> <pre>select count(*) from sys.aud\$.</pre> <p>On an upgraded system, run the following sql statements as oracle user to disable audit:</p> <pre>cd \$ARCSIGHT_HOME/bin ./arcsbutil sql / as sysdba NOAUDIT CREATE SESSION; exit</pre>

ArcSight Manager

Issue	Description
ESM-50704	<p>Previously, an export would fail to complete using the package command. This is now fixed. Now it can export large packages using the CLI command in standalone mode.</p>
ESM-46773	<p>In this release there is an added option in the email format to compress a scheduled report before emailing. The option is, 'Attach Compressed Report,' under Report Parameters.</p> <p>The new feature is documented in the What's New for ESM 5.5, and in the ArcSight Console User's Guide, in the "Building Reports" topic under the subtopic "Report Parameters: Default and Custom."</p>
ESM-34014	<p>System automatically deactivates any user account that has been inactive for more than 90 days. After installing the product, run the "arcsight managersetup" command to implement this feature. Then restart the Manager.</p> <p>To change the inactive period, add the property auth.user.account.age= <days> to the Manager's server.properties file, change <days> to the number of days you want, and restart the Manager.</p> <p>This behavior is now documented in the "Managing Users and Permissions" topic of the ArcSight Console User's Guide.</p>
ESM-30314	<p>The ArcSight Console Guide topic Modeling the Network > Auto Zoning an Asset now states that you cannot move an asset using Auto Zone if the asset is locked.</p>

ArcSight Web

Issue	Description
ESM-50148	Previously, there was a security issue that session cookies for ArcSight Web were set on the client web browser without the HTTPOnly directive enabled. This has now been fixed.
ESM-49935	Previously, the exception stack would display in the page source. This is now fixed by the addition of a new property. To NOT display the exception stack in page source, add the following property in webserver.properties: web.display.exception.stack=false Then clear the browser cache. This is now documented in the "Preferences" section of the ArcSight Web User's Guide.

Installation and Upgrade

Issue	Description
ESM-50466	While setting up Partition Archiver in Suite B mode, the setup wizard might fail with a pop up error dialog. To resolve this problem: 1. Close this error dialog and click Cancel to exit the agent setup wizard. 2. Create or edit the <ARCSIGHT_HOME>/user/agent/agent.properties file and add the following line to this file: fips.enabled=true 3. Run "arcsight agentsetup" again to register the Partition Archiver.
ESM-50390	The ESM Installation & Configuration Guide now contains an important clarification with respect to running the Partition Archiver as a service. The recommendation is: "ArcSight recommends that you install Partition Archiver as a service and do not change the default values unless necessary. Partition Archiver must be run as the Oracle software owner (that is, oracle, by default) on UNIX and as a user (Administrator, by default) on Windows in the local user group ORA_DBA."

Open Issues in 5.5

Analytics

Issue	Description
ESM-50625	If the name of a Session List contains the ampersand (&) character, creating a rule action AddToSessionList on this Session List produces an error. The workaround is to avoid using an ampersand in Session List names.
ESM-49436	Filters having conditions on Variables that return an Actor list field cannot be used in Queries and Active Channels. You can only use these filters in Rules and Data Monitors. This issue affects content developers using Variables in ESM.

Issue	Description
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-47918	The Threat Response Manager (TRM) occasionally does not return an appropriate response when an update to Quarantine Node by IP command is sent.
ESM-40529	After installing IdentityView 1.1, some previously valid ESM resources show as invalid resources. Workaround: Edit the filter called Built In Identities on IDM System and remove the setAction local variable.
ESM-40449	When exporting events from the Case Details channel, archived events do not get exported.
ESM-39632	The copy-and-paste function is not supported for conditions with variables. For example, if you create a filter for an Active Channel and used the Common Conditions Editor to add condition statements, copying and pasting into another editor (for example, a Rule editor) may result in an error. Workaround: Manually re-enter the conditions.
ESM-38902	Importing or exporting domain fields show these fields to be Unknown Fields in the rule editor. Workaround: While importing or exporting, make sure to include the domain field set to which the domain fields belong.
ESM-37810	For scheduled reports, when the user's "Run as" read and write privileges are taken away, the scheduled report is generated by the user who created the schedule (and not by the "Run as" user). If the "Run as" user has read privilege only, then the report is not generated.
ESM-35070	Verify Rules with Events (replay with rules) does not work for the following types of active lists if one of the rules adds to the active list and the second rule uses that data in a condition: - An event-based active list with values - A field-based active list with values, where all fields are mapped to event fields Verify Rules with Events does work for other types of active lists and when only one rule is used. Also, valid active lists work properly with real-time rules when they are deployed, including the two types of active lists described above.
ESM-34531	When you set the Schedule Frequency for a report, the Next Run Time field is displayed incorrectly in the Editor. Even though the time is displayed incorrectly, the report runs at the time specified in the editor.

Issue	Description
ESM-33525	<p data-bbox="493 258 1364 441">Variables in some conditional statements in query definitions are improperly translated. Variables in GROUP BY and SELECT expressions are translated as CASE statements, and this causes problems in the GROUP BY part of the query definition. (The GROUP BY should be using the alias given to CASE statements in the SELECT statement, but this is not working properly.) Running a report or launching a Query Viewer with such a query generates an exception similar to this one:</p> <p data-bbox="521 455 1091 476">The query run failed because of the following reason:</p> <p data-bbox="493 491 1273 541">com.arcsight.common.ArcSightException: com.arcsight.common.introspection.queryable.QueryableFetchException:</p> <p data-bbox="493 556 1364 606">Encountered persistence problem while fetching data: Unable to execute query: ORA-00979: not a GROUP BY expression</p> <p data-bbox="493 621 1364 672">Conditional variables in a SELECT statement with an aggregated field causes an Oracle exception (not a GROUP BY expression)</p> <p data-bbox="493 686 631 707">Workaround:</p> <ol data-bbox="493 722 1219 781" style="list-style-type: none"> 1. Remove the ORDER BY fields in the Query resource. 2. Use the sort options provided by the Query Viewer or the Report.
ESM-29633	<p data-bbox="493 804 1364 854">Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid.</p> <p data-bbox="493 869 1364 970">Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (For example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.</p>
ESM-29348	<p data-bbox="493 993 1364 1283">The Scheduled Time column in the Scheduled Runs view covers both time ranges for runs that have already occurred and for runs that are pending. As a result, you will see some discrepancy in the time ranges shown in the column. For example, against the runs that have already occurred, you will see the lower end of the time range. (For trends set to run hourly, if the time range is between 1:00 pm - 2:00 pm you will see 1:00 pm). The pending runs show the upper range (if the time range is between 1:00 pm - 2:00 pm you will see 2:00 pm). Trends that have already occurred will have a time difference that reflects the trend query schedule (for example, one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (for example, 24 hours if run once a day).</p>
NGS-4184	<p data-bbox="493 1306 1364 1520">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 data-bbox="493 1535 1341 1585">Workaround: We recommend that you specify a positive timeout value for only one negated alias, and set the remaining timeouts to zero.</p> <p data-bbox="493 1600 1281 1650">This is documented in the "Negating Event Conditions" topic in the "Rules Authoring" section of the ArcSight Console User's Guide.</p>

Issue	Description
NGS-2843	<p>With new packages, by default, system resources are excluded if not explicitly included. However, with older packages created before the new default package exclusions, it is possible that packages will include system resources. When these packages are deleted from the system, with the option to delete the resources selected, it is possible to delete system resources that are not locked or not in locked groups. This can cause some serious issues, especially when the system resources in question are Zones.</p> <p>If this happens, the package should be re-imported and modified to exclude the system resources, then deleted again. Alternatively, the package can be re-imported, then all the desired resources manually deleted, and lastly delete the package with the "leave resources" option.</p>

ArcSight Console

Issue	Description
ESM-51005	<p>When a user logs into the console and if the password is expired, an exception as following may occurs in an pop up box:</p> <p>Exception caught while logging in to core service: class java.io.IOException</p> <p>Workaround: Click OK, and it will allow you to continue with normal operation.</p>
ESM-48908	When viewing custom layout dashboards in an external browser, the Show Events menu option will not launch the Event Inspector.
ESM-47495	Custom Layout Dashboards now support Query Viewers, however, the toolbar in each dashboard and the left-click context menus still use the "Data Monitor" menu label, although Query Viewers are also available from this link.
ESM-47489	<p>If you add a Query Viewer with a default row limit of 10,000 to a dashboard, the dashboard may not load in Custom Layout. The reason is that the Custom Layout is web based and requires a web browser to work. Most web browsers can't handle such large amount of data.</p> <p>Workaround: Reduce the row limit before adding the Query Viewer to the dashboard.</p>
ESM-47386	A Query Viewer can be added to a dashboard displayed as a stacked bar chart. However, if this dashboard is displayed in Custom Layout, you will see a regular bar chart because the stacked bar chart is not supported in this release in Custom Layout.
ESM-47213	<p>Case-related events are copied to a special table so they can remain available after being archived. The channel is unable to find and display such events correctly after the partition is archived.</p> <p>Workaround: Use the case event editor or Reports, which can correctly find and display these events.</p>
ESM-41641	<p>On 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-41344	<p>When viewing image dashboards in an external browser, if you keep the dashboard running, you will get an error saying that a script on the page is causing the browser to run slowly and if it continues to run, your computer may become unresponsive. This error appears after every few hours while the image dashboard is running.</p> <p>Workaround: Click No to dismiss the message. You may also refresh the page.</p>

Issue	Description
ESM-41247	<p>If you set "NSPAuth" as Password type and run TRM commands in the external browser, you will be redirected to the Login page.</p> <p>Workaround: Set NSPAuth to Text type if you want to use the external browser for TRM commands. One issue with this workaround is that the authentication token would appear as clear text in your browser URL parameters.</p>
ESM-41019	<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 product 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 Administrator's Guide for details on how to do this.</p>
ESM-40302	<p>On an ESM running in FIPS mode, the server.log file shows an exception when a Custom View dashboard is launched. This is because Custom View dashboards are not supported in FIPS mode.</p>
ESM-39980	<p>The Console can become unresponsive if you access other resources while building category models with a large number of actors.</p>
ESM-39856	<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	<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>
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>
ESM-38961	<p>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.</p> <p>Workaround: After the upload, move the file to a preferred folder.</p>
ESM-38014	<p>When a filter is moved from one group to another and data monitors that depend on that filter are packaged, exported, and re-imported on a different ESM installation, the data monitors may lose some filter attribute values.</p> <p>Workaround: Manually specify the filter again for data monitors that are identified by the broken resource icon.</p>
ESM-37868	<p>When you modify a case while a case channel is open and an inline filter is applied, no data appears.</p> <p>Workaround: To successfully display available data, refresh the case channel.</p>
ESM-37344	<p>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.</p> <p>Workaround: Arrange the resource hierarchy so there are no more than 1000 resources in a single group. Alternatively, use a dynamic case name (a case name that includes a variable).</p>

Issue	Description
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, 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-34830	On the ESM Console, the Connector configuration settings do not support decimals for the "Limit event processing rate" option (only integer settings are supported for this release), even though decimals are supported for this option on the Connector. Right-click the connector and choose Configure. Select Default > Content > Processing.
ESM-33440	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-33360	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	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-32489	Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.
ESM-30791	On Macintosh: If you click the Help menu and select About and then click the ArcSight Copyrights... link in the "About" page, you will get a Java Exception. This exception is generated by an issue in the Grand-Rapid browser.
ESM-27970	Searching for Resource IDs (such as the Resource IDs for Trends and Queries) returns an error when they begin with non-alphanumeric characters. To search for such Resource IDs, enclose the ID in double quotes. For example, to search for <code>^VVsOXg4BABCAIEuBhILMyg==</code> Enter <code>"^VVsOXg4BABCAIEuBhILMyg=="</code> in the query text field.
ESM-26488	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. 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.

ArcSight Database

Issue	Description
ESM-50367	<p>During installation, you specify the size, path to, and number of files for each tablespace. Oracle adds up the total space requirement and checks to see if there is sufficient space to install them. If there isn't, the install fails.</p> <p>On Unix-based operating systems, if you choose to install different tablespaces in different partitions, mount them at the root directory.</p> <p>If you have not, Oracle checks the total size of all tablespaces against each partition and, if there is not enough space for all of them in any one partition, the install fails.</p> <p>There are two ways to get around this:</p> <ul style="list-style-type: none"> - Mount these partitions at the root directory before you install. - Set the table spaces small enough so that all of them fit into each of the partitions you plan to use. Then, after the installation, use the arcsight database xts command to expand the tablespace sizes to the desired size. <p>This is documented in the Installation Guide topic at "Installing ArcSight Database > General Guidelines for Installing Oracle > Storage Guidelines > Disk Space Requirements > Placing Tablespaces in Separate Partitions"</p>
ESM-49915	<p>There is an Oracle vulnerability for which there is a documented workaround you should use.</p> <p>Refer to the Knowledge base article at http://support.openview.hp.com/selfsolve/document/KM1388068.</p>
ESM-48270	<p>There is a performance issue when running channels or queries with conditions on actor global variables.</p> <p>Workaround: The following tips might be helpful in improving performance.</p> <ol style="list-style-type: none"> 1. Generate session list statistics as follows: <p>Run the following three commands in <ARCSIGHT_HOME>\bin on your database machine:</p> <pre>./arcdbutil sql username/password @../utilities/database/oracle/common/sql/runSessionListStats.sql exec runSessionStats</pre> <p>The runSessionStats command gathers statistics on all session list tables and gathers both global- and partition-level statistics. You should see an improvement in performance.</p> <p>Note that the scripts may run for a long time if the session lists have a lot of data.</p> 2. You could also reduce the rownum limit from the default of 10,000 to 1000 or lower to improve the data retrieval time. 3. If the actor query has joins to event-related tables, then running RegenerateEventStats (described in the "Query and Trend Performance Tuning" section) helps to improve the overall read performance of the system. This may take from a few minutes to a few hours, depending on the volume of events. 4. Eliminating the LIKE condition from the query will extensively improve the query performance.

Issue	Description
ESM-48248	<p>Some solutions, system or customer reports that executed correctly on Oracle 10g, may fail on Oracle 11g with the error "Unable to execute query: ORA-00979: not a GROUP BY expression."</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Log in to Oracle as "sysdba". 2. Run the following SQL command from the sqlplus prompt: alter system set "_optimizer_distinct_agg_transform"=false scope=both; 3. Restart Oracle to apply the change to all sessions.
ESM-46556	<p>During the Oracle database installation, when you create a database instance, when specifying the ORACLE_SID, the wizard does not warn you if you use a name with a space (for example, esm db).</p> <p>Oracle does not allow spaces and therefore the instance creation will fail if the ORACLE_SID (instance name) has a space in it. Do not use spaces in this string.</p>
ESM-35620	<p>The ArcSight Database installer does not include error checking or validation against Oracle-supported schema user naming conventions. If the user names specified contain anything other than alphanumeric characters, the ArcSight Database installer will prevent creation or re-creation of the schema and will display the following error code:</p> <p>error ORA-00921: unexpected end of sql command</p> <p>Workaround: For ArcSight Database installation and schema setup, keep in mind that Oracle supports only alphanumeric characters for database user names, and will not accept a dash (-) or underscore (_) in these names.</p>
ESM-34568	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <p>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</p> <p>This occurs because Oracle is using a sub-optimal query execution plan. In some cases, this can happen because of insufficient space in the ARC_TEMP table.</p> <p>Workaround: Set the report to query with a full scan database hint. For more information, refer to the section, "Reports that query over a large time range with complex joins take a long time to run" in Appendix B of the ArcSight ESM Administrator's Guide.</p>

ArcSight Manager

Issue	Description
ESM-48784	<p>If a customer name contains the special character double quotes " " in the OU (Organization Unit) the user does not get processed correctly when translated to a URI. When this happens, it prevents the respective Actor name from getting created in the group correctly (wrong name and wrong group).</p>

Issue	Description
ESM-41331	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: To produce a correct report, run the resource validation script manually as follows:</p> <ol style="list-style-type: none"> 1. Run the script using 'arcsight resvalidate' 2. Run the script again using 'arcsight resvalidate -persist false' <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	<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-37633	<p>After installing the Manager, you will see an error in the server.log file:</p> <pre>[ERROR][default.com.arcsight.config.util.WebProperties][getPassword] com.arcsight.common.ArcSightException: Cannot handle the data which was obfuscated by old scheme</pre> <p>This message is harmless and can be safely ignored.</p>
ESM-37488	<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	<p>Stages resources are editable from the ArcSight Console, although these should not be moved or customized. (See the ArcSight 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-33431	<p>When upgrading some older versions of ESM with Oracle 10G, you may see some negative timestamp values in the server logs. You will see an error that begins with "java.sql.SQLException: BC date found in..." in the logs. The resources for this error are not loaded.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Set the following property in the Manager's <ARCSIGHT_HOME>/config/server.properties file: server.date.correction.recoverFromBCDate=true 2. Restart the Manager. <p>Should this issue occur, notify Customer Support.</p>

Issue	Description
ESM-31433	<p>You may see the following exception in the Manager's log file:</p> <p>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</p> <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	<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-30008	<p>Occasionally, when installing an exported package from a bundle file, you might receive the following error:</p> <p>Install Failed: Resource in broker is newer than modified resource.</p> <p>This error does not occur every time you attempt to install an exported package from a bundle.</p> <p>Workaround: Re-import the package.</p>

ArcSight Web

Issue	Description
ESM-35801	<p>If you create a Case and set the Estimated Resource Time in ArcSight Web, it does not get set.</p> <p>Workaround: Define this setting on the Console. See the Console online Help for steps to do this.</p>
ESM-35693	<p>If your session has expired and you click a node in the Navigator tree to expand it, you will see a Java exception and ArcSight Web does not redirect you to the login page.</p> <p>Workaround: Start a new session and log in again.</p>

Issue	Description
ESM-33922	<p>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 hard to read.</p> <p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 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	<p>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:</p> <p>http://www.adobe.com/go/6b3af6c9</p>

Installation and Upgrade

Issue	Description
ESM-50200	<p>On Windows, when upgrading from Oracle 11.2.0.2 to 11.2.0.3, if Oracle 11.2.0.2 is installed on any drive other than the C: drive, it can cause access denied errors. Follow this procedure before you start the installation:</p> <ol style="list-style-type: none"> 1. Shutdown the Oracle Services. (This is a specific exception to the warning against doing this in Upgrade section.) 2. Set the environment variable <code>ORACLE_HOME</code> to the current path to your Oracle installation, if it isn't already set. (This causes the installer to create a <code>.backup</code> directory.)
ESM-51033	<p>When you install Forwarding Connector 5.1.7. 6151 on Linux 6.1, Linux 6.2, or Aix 6.1 you get the following error message:</p> <p>"You are installing this product on an unsupported platform. See the SmartConnector Configuration Guide for your device for specific information about this message."</p> <p>You may click OK and ignore this message.</p>

Issue	Description
ESM-51012	<p>During the Oracle instance upgrade (that is, after you have installed Oracle 11.2.0.3), at the point of 'Performing post-upgrade tasks', you may see an error message as follows:</p> <p>"We cannot connect to the upgraded Oracle 11.2.0.3 instances. Please verify that the Oracle instance and TNS listener are up."</p> <p>If the Oracle instance and listener are actually up and running, the error can be safely ignored. To verify they are running, issue the following commands in the <ARCSIGHT_HOME>/bin directory to complete the post-upgrade process:</p> <p>In a command prompt, run:</p> <pre>arcdbutil listener status</pre> <p>Check that the command returns no errors. Then run:</p> <pre>arcdbutil sql <user>/<pass>@tnsnames</pre> <p>...where <user>/<pass> are the Oracle user ID and password and tnsnames is arcsight (by default). This command should complete the connection, thus completing the post-upgrade process.</p> <p>Click OK on the error message and then, because the post-upgrade process is now complete, click Cancel on the wizard screen.</p>
ESM-50891	<p>When upgrading from ESM 5.2 P2 to ESM 5.5, the Manager configuration runs the commands dbcheck and system_export_tables. However, after running the system_export_tables command, it does not create arcsight.dmp file on Windows. As a workaround, use following commands to create the dump file:</p> <pre>cd %ARCSIGHT_HOME%\bin</pre> <p>open the file named system.param</p> <p>remove the two lines that starts with old and new like below.</p> <p>old 1: select table_name ',' from user_tables where tablespace_name='ARC_SYSTEM_DATA' and table_name <> 'PLAN_TABLE' &1 '&2'</p> <p>new 1: select table_name ',' from user_tables where tablespace_name='ARC_SYSTEM_DATA' and table_name <> 'PLAN_TABLE' and upper(table_name) not like 'ARC_SLD_%'</p> <p>Save the file.</p> <pre>cd <ARCSIGHT_HOME>\bin</pre> <pre>expdp <username/password@instance> directory=ARCSIGHT_DUMP_DIR dumpfile=arcsight.dmp parfile=<ARCSIGHT_HOME>\system.param</pre>
ESM-50787	<p>There is a problem when trying to install Oracle and creating a database instance with a new SID name, such as, for example, "hpcloud". After the Oracle database instance is created, when you try to connect to the database instance, it will connect to the instance name with its previous alias name which is "arcsight". This causes the Manager upgrade to fail because before upgrading the manager, it has to export the system tables, and it does so with the "arcsight" alias name. But the Manager upgrade process is exporting the system tables with "hpcloud" SID.</p> <p>The workaround is to change the alias name from "arcsight" to "hpcloud" in tnsnames.ora</p>
ESM-49566	<p>The Case schema customized settings are not transferred over during upgrade. Please contact Customer Support for help with transferring the Case customization settings.</p>

Issue	Description
ESM-49396	<p>While upgrading the Manager in console mode, when prompted:</p> <p>Continue [yes] ?</p> <p>you will see unrelated messages on the standard output, which can be confusing. Ignore the messages regarding building of rules. They come from another thread. Answer only the last prompt that you receive during the upgrade. For example, when you see the following, type "yes".</p> <p>Continue [yes] ?Building the rule Monitor New Case</p> <p>Building the rule Case Deleted</p>
ESM-41148	<p>During ESM upgrade, autozoning will fail if the number of assets in a zone/group exceeds 1000.</p> <p>Workaround: Manually run autozoning in batches of 1000 assets or fewer after completing your upgrade. You can do this from the Asset Channel or Asset Resource Tree in the Console.</p>
ESM-40984	<p>Before uninstalling any ArcSight package, certain tasks must be performed in sequence. Remove relationships first before deleting. For example, if the data monitor group is deleted before the data monitor resource, you will encounter a permission error, because permissions are tied to groups.</p>
ESM-35653	<p>ESM Console upgrades do not properly read the security and login property settings (SSL files). If you run the upgrade and Console setup through to completion via the install wizard, you will still have to re-run Console setup.</p> <p>Workaround: Cancel the installation after the Console is installed, and run the ArcSight Console Configuration Wizard to configure property settings. From the Console's <ARCSIGHT_HOME>/current/bin, run the command,</p> <p>arcsight consolesetup</p> <p>The SSL files will be read and the Console will configure correctly.</p>

Pattern Discovery

Issue	Description
ESM-35048	<p>A java.lang.InterruptedException might be logged in the Manager's server.std.out.logs file when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.</p>

