

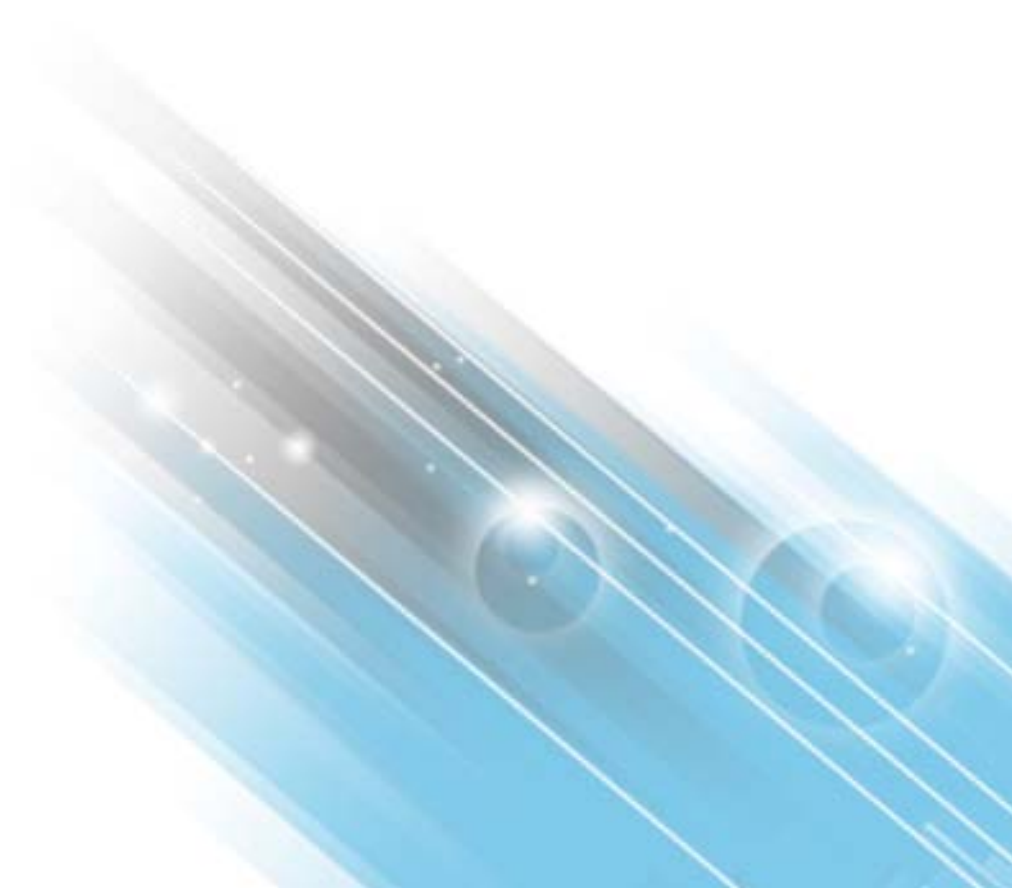


# HP ArcSight ESM

Software Version: 5.6

## Release Notes

September 20, 2015



Copyright © 2015 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>

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

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

This document is confidential.

## Contact Information

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

## Revision History

Date	Product Version	Description
09/20/2015	5.6	Release Notes for ESM 5.6 release.

# Contents

---

<b>ArcSight ESM Version 5.6 .....</b>	<b>5</b>
Welcome to ArcSight ESM Version 5.6 .....	5
What's New in This Release .....	5
Oracle Support .....	5
POODLE Fix .....	5
Oracle PSU .....	6
Upgrade Support .....	6
Geographical Information Update .....	6
Vulnerability Updates .....	6
Usage Notes .....	7
Forwarding Connector .....	7
Browsers and Custom View Dashboards .....	7
JRE on Macintosh .....	7
Oracle Enterprise Manager Issue .....	7
Fixed Issues in 5.6 .....	8
Analytics .....	8
ArcSight Console .....	8
Documentation .....	9
ArcSight Database .....	9
ArcSight Manager .....	9
Open Issues in 5.6 .....	11
Analytics .....	11
ArcSight Console .....	11
ArcSight Database .....	15
ArcSight Manager .....	16
ArcSight Web .....	18
Installation and Upgrade .....	18



# ArcSight ESM Version 5.6

---

## Welcome to ArcSight ESM Version 5.6

ArcSight Enterprise Security Management (ESM) 5.6 provides updates to Oracle, Red Hat Linux, and CentOS support.

If you are planning on migrating to ESM with CORR-Engine, do not install ESM 5.6. Instead, migrate ESM 5.5 to ESM with CORR-Engine.

## What's New in This Release

This section contains a summary of the improvements and new capabilities introduced as part of the ArcSight ESM 5.6 release.

New in this release:

- ESM 5.6 now supports Oracle 11.2.0.4.
- ESM 5.6 now supports new versions of RHEL, CentOS, Windows Server 2012, and Mac OS 10.9 (for ArcSight Console). See the ESM Support Matrix for platform support details.
- The security vulnerability known as "Padding Oracle On Downgraded Legacy Encryption" (POODLE) has been fixed.
- Addresses critical issues in ESM 5.5.
- Provides updates for geographical information and vulnerability mapping.
- Provides important security updates.

## Oracle Support

ESM 5.6 uses Oracle 11.2.0.4. If you are using Oracle 11.2.0.3, you can upgrade to Oracle 11.2.0.4 after upgrading the ArcSight Database component. In the Upgrade Guide, see the chapter "Upgrading Oracle Database," for details on how to upgrade Oracle.

## POODLE Fix

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit that takes advantage of Internet and security software clients' fallback to SSL 3.0. See <http://en.wikipedia.org/wiki/POODLE> for details.

When establishing SSL connection in Java, applications start from protocol negotiation (SSL, TLS, TLSv1, etc.). The POODLE SSL fix ensures that no instance of ESM or ArcSight Web will accept connections of SSLv3 type; only TLS protocols are accepted. The corresponding changes were made to the ArcSight Console, which is one of the ESM clients. No additional changes are required for the ArcSight Console. To access ArcSight Command Center the web-browser should allow the use of TLSvx protocols, which is the default setting for all web browsers.

## Oracle PSU

Refer to the latest ArcSight Oracle Patch Set Update (PSU) Release Notes for Oracle Patch Set Update (PSU) and OPatch information. You must install the latest PSU after upgrading Oracle.

## Upgrade Support

The upgrade path that is supported for this release is ESM 5.5 Patch 2 to ESM 5.6

Please refer to the upgrade guide for more information on upgrade instructions.

## Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532\_20150701.

## Vulnerability Updates

This release includes recent vulnerability mappings (July 2015 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 1321 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Enterasys Dragon IDS updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S876 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Juniper / Netscreen IDP update 2511 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, MSSB, CERT
McAfee Intrushield updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, CERT, MSSB
TippingPoint UnityOne DV8730 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
IBM Enterprise Scanner 1.134 updated	CVE, X-Force
IBM Security Host Protection for Desktops 3150 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 35.070 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3150 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 35.070 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 35.070 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Server IPS for Linux technology 35.070 updated	Faultline, CVE, Nessus, X-Force

Device	Vulnerability Updates
IBM RealSecure Server Sensor XPU 35.070 updated	Faultline, CVE, Nessus, X-Force
Symantec Endpoint Protection updated	Faultline, Bugtraq, CVE, X-Force, Nessus
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	Bugtraq

## Usage Notes

Please review the following points to ensure smooth operation.

### Forwarding Connector

The Forwarding Connector can receive events from a source Manager and then send them to a secondary destination Manager, a non-ESM location (such as HP Operations Manager), or to an ArcSight Logger. The Forwarding Connector to install for ESM 5.6 is version 7.1.3.7495.0. See the ESM Support Matrix document available on the Protect 724 site for details on ESM 5.6 supported platforms.

### 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 64-bit and 32-bit browsers:

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

### JRE on Macintosh

On the Macintosh 10.9 platform, install JRE 1.6.0\_65 before installing ESM 5.6.

### Oracle Enterprise Manager Issue

After an Oracle upgrade or fresh install, it is possible that either:

- The wrong Oracle version number appears on the home tab, or
- The Oracle Enterprise Manager fails to start at all.

If either issue occurs, contact Customer Support.

If you are running Oracle on Red Hat 7.0 or 7.1, you must download the patch for OEM for Oracle 11.2.0.4 on Red Hat 7.x from <http://softwaresupport.hp.com>

## Fixed Issues in 5.6

### Analytics

Issue	Description
ESM-51604	When a user attempted to modify a rule without read permissions to all rules, the modification appeared to succeed but was not actually applied. This has been fixed.
ESM-51379	Queries used in the report or query viewer or channel have a performance issue when there is a large amount of event annotation data. This fix resolves this issue by optimizing the query time dynamically.  Workaround: Enable the event.annotation.optimization.enabled property in the server.properties file. When this property is set to true, the new optimization is enabled. Note that, default optimization occurs unless you set event.annotation.optimization.enabled to true. You do not have to set event.annotation.optimization.enabled in the server.properties file unless you need the dynamic query time optimization.  This functionality is certified for a stand-alone deployment only. Other limitations apply. Contact HP Technical Support with any concerns.
ESM-51353	When rule modification was done by user who did not have read access to all the rules, the modification appeared to succeed, but was not applied. This issue is now fixed in this release.
ESM-51337	In some situations, the requestUrlHost field was not derived properly from the fully-qualified request URL. This issue has been fixed.
ESM-50574	On ESM 5.2 with RHEL 6.1, you would get a "Wrong exit code '1'" error when perl is configured as an external command of a Rule Action. This is now fixed.

### ArcSight Console

Issue	Description
ESM-51500	If a case's description tab were opened by two Consoles simultaneously, updates made by one console were not visible in the other console after properly unlocking the case, unless the case was closed and re-opened. This has been addressed.
ESM-51107	Modifying the fieldset of an Active Channel (AC) using Customize Columns will now show data in a field added to channel.
ESM-50790	When querying for cases based on case owner, the system required usage of the resource id, not the name. This has been fixed.
ESM-50400	For one specific Target Geo location, the IP resolved to 0,0. This has been fixed.

## Documentation

Issue	Description
ESM-51443	<p>ESM v5.2 and ESM v5.5 Installation Guides under section titled "Migrating from Internal Authentication to ACE/Server" have this note: "If you are switching from the internal authentication mechanism to ACE/Server after the initial installation and the external user ID of all administrator accounts is different from the internal user ID, contact HP for assistance in setting the external ID for administrator user accounts. " Later in these guides, we explained this step clearly in section titled "Guidelines for setting up external authentication."</p> <p>In ESM 5.6 this note has been changed to as follows, "If you are switching from the internal authentication mechanism to ACE/Server after the initial installation, and the external user ID of all administrator accounts is different from the internal user ID, see 'Guidelines for setting up external authentication' on page 92."</p>

## ArcSight Database

Issue	Description
ESM-51499	<p>When upgrading Oracle 11.2.0.2 to 11.2.0.3 on SuSE, the version reported was incorrect. After upgrading Oracle from 11.2.0.3 to 11.2.0.4 and applying the April 2015 PSU, the version reported is correct on SuSE.</p> <p>This issue has been fixed.</p>
ESM-51274	<p>After applying the October 2013 Oracle Patch Set Update, Isnrctl start failed with Linux Error 29: Illegal seek. This has been fixed in the latest release of Oracle, 11.2.0.4.</p>
ESM-51220	<p>Partition Compression could fail with an ORA-00600 error code. This has been resolved in version 11.2.0.4 of the database.</p>
ESM-50922	<p>There was an export issue in a particular customer large db environment.</p> <p>The export issue was resolved with the workarounds and scripts by exporting the db dump files into a few smaller files.</p> <p>A KB article is created for this issue. Please contact Tech Support for detail instructions.</p>

## ArcSight Manager

Issue	Description
ESM-51608	<p>Annotating events took a long time to come back and froze the console. This problem is now fixed in this release.</p>

Issue	Description
ESM-51579	<p>This Patch release provides the POODLE SSL fix.</p> <p>The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit that takes advantage of Internet and security software clients' fallback to SSL 3.0. See <a href="http://en.wikipedia.org/wiki/POODLE">http://en.wikipedia.org/wiki/POODLE</a> for details.</p> <p>When establishing SSL connection in Java, applications start from protocol negotiation (SSL, TLS, TLSv1, etc.). The POODLE SSL fix ensures that no instance of ESM or ArcSight Web will accept connections of SSLv3 type; the protocol should be one of TLS protocols. The corresponding changes were made to the ArcSight Console, which is one of the ESM clients. No additional changes are required for the ArcSight Console. To access ArcSight Command Center the web-browser should allow the use of TLSvx protocols, which is the default setting for all web browsers.</p>
ESM-51526	<p>The CFC could cause the source ESM to drop its EPS by a significant amount, especially when the initial EPS was high.</p> <p>CFC no longer affects EPS.</p>
ESM-51433	<p>Attempting to search a large number of Assets or Zones in Console failed due to exception. This has been corrected, so such searches will successfully yield data.</p>
ESM-47652	<p>The newids parameter in the archive tool does not assign new ids to resources.</p> <p>The newids parameter does not function and is no longer documented.</p>

## Open Issues in 5.6

### Analytics

Issue	Description
ESM-49436	<p>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.</p> <p>This issue affects content developers using Variables in ESM.</p>
ESM-48858	<p>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.</p>
ESM-47918	<p>The Threat Response Manager (TRM) occasionally does not return an appropriate response when an update to Quarantine Node by IP command is sent.</p>
ESM-40529	<p>After installing IdentityView 1.1, some previously valid ESM resources show as invalid resources.</p> <p>Workaround: Edit the filter called Built In Identities on IDM System and remove the setAction local variable.</p>
ESM-39632	<p>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.</p> <p>Workaround: Manually re-enter the conditions.</p>
ESM-38902	<p>Importing or exporting domain fields show these fields to be Unknown Fields in the rule editor.</p> <p>Workaround: While importing or exporting, make sure to include the domain field set to which the domain fields belong.</p>
ESM-37810	<p>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.</p>
ESM-29633	<p>Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (for example, you could toggle the trend's enabled state off and then back on) and then save it. This will force the re-validation of the trend and re-enable the trend.</p>

## ArcSight Console

Issue	Description
ESM-51881	<p>There are some residual links and files after the uninstall of ESM 5.6 console on Mac OS X 10.9.</p> <p>To clean up these files execute the standard Unix delete commands.</p>

Issue	Description
ESM-51865	<p>Logging in to the ESM 5.6 Console using the 'PKCS#11 Login' option can generate an error message of: 'Failed to connect to the PKCS#11 Token' on Windows 64-bit.</p> <p>Follow the workaround below to resolve this known JDK6 issue:</p> <ol style="list-style-type: none"> <li>1. Copy C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll to a new folder (e.g. C:\arcsight\ActivClient)</li> <li>2. Edit the ESM Console's client.properties by inserting this line to the file: cac.pkcs11.lib=C:\arcsight\ActivClient\acpkcs211.dll</li> <li>3. Re-start Console and you should be able to login with the PKCS#11 option.</li> </ol>
ESM-51005	<p>When a user logs into the console with an expired password, the following exception may occur in an pop up box after entering a new password:</p> <p>"Exception caught while logging in to core service: class java.io.IOException."</p> <p>The workaround is to click OK, and it will allow you to continue normally.</p>
ESM-48908	<p>When viewing custom layout dashboards in an external browser, the Show Events menu option will not launch the Event Inspector.</p>
ESM-47495	<p>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.</p>
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	<p>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.</p>
ESM-47213	<p>For ESM with the Oracle database, 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-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>
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>

Issue	Description
ESM-41019	<p>When you have client-side authentication set up, and if the Manager is configured with the Password Based and SSL Client Based Authentication, an error will be returned when accessing the product documentation using a Web browser.</p> <p>Workaround: Generate a key pair for the browsers and import the browser's certificate into the Manager's trust store. Alternatively, copy the Console's key into the browser's keystore. See the Administrator's Guide for details on how to do this.</p>
ESM-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 should only take a few seconds. However, when thousands of actors are deleted, the cumulative deletion period may last for hours.</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> <p>Workaround: To view additional fields in an Actor channel, add the fields to an Actor field set and use it in the actor channel.</p>
ESM-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 ArcSight Console, when a large number of cases reside in a single group, you can't pick a case for the "Add to Existing Case" rule action in the Rule editor. This is because the resource selector only shows leaf nodes when there are less than 1000 cases in a group. This happens for all resources.</p> <p>Workaround: Arrange the resource hierarchy so there are no more than 1000 resources in a single group. Alternatively, use a dynamic case name (a case name that includes a variable) in your rule action to specify the case. In the ArcSight Console User's guide, search for "Dynamic case name" in the "Rules Authoring" chapter.</p>
ESM-36055	<p>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, when such query is used in query viewer or report it will not show data.</p>
ESM-32489	<p>Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.</p>

Issue	Description
ESM-30008	Installing an exported package from a bundle file occasionally results in the following error: Install Failed: Resource in broker is newer than modified resource. Workaround: Re-import the package.
NGS-11209	On Mac OS X only: If you open a channel, select some rows, right-click on them and select Print Selected Rows from the resulting menu without a default printer set up, the Console will abruptly terminate. Workaround: Before you start the Console, make sure to set up a default printer to which to print.

## ArcSight Database

Issue	Description
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-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 <a href="http://support.openview.hp.com/selfsolve/document/KM1388068">http://support.openview.hp.com/selfsolve/document/KM1388068</a>.</p>
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"> <li>1. Log in to Oracle as "sysdba".</li> <li>2. Run the following SQL command from the sqlplus prompt:  <pre>alter system set "_optimizer_distinct_agg_transform"=false scope=both;</pre> </li> <li>3. Restart Oracle to apply the change to all sessions.</li> </ol>
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-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"> <li>1. Set the following property in the Manager's &lt;ARCSIGHT_HOME&gt;/config/server.properties file:  <pre>server.date.correction.recoverFromBCDate=true</pre> </li> <li>2. Restart the Manager.</li> </ol> <p>Should this issue occur, notify Customer Support.</p>

## ArcSight Manager

Issue	Description
ESM-51851	<p>When using Internet Explorer 11 with FIPS mode, the browser is unable to access Manager port 8443 and Web port 9443.</p> <p>Workaround: Use a different browser.</p>
ESM-40889	<p>The "group:101" audit event might not be sent when there are many role memberships being added or changed for an actor. An error about this is written to the server log, indicating the IDs of the affected objects.</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"> <li>1. Generate session list statistics as follows:           <p>Run the following three commands in &lt;ARCSIGHT_HOME&gt;\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> </li> <li>2. You could also reduce the rownum limit from the default of 10,000 to 1000 or lower to improve the data retrieval time.</li> <li>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.</li> <li>4. Eliminating the LIKE condition from the query will extensively improve the query performance.</li> </ol>
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-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>Exporting a large active list with 10 million entries, or exporting rules that use such active lists, results in an exception in the server.std.log file. Additionally, the Manager runs out of memory and automatically restarts itself.</p> <p>Workaround: Use the export format instead of the default format while exporting the rule or active list definition using an archive or a package.</p>

Issue	Description
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 &lt;ARCSIGHT_HOME&gt;/current/bin, run the command:</p> <pre>arcsight consolesetup</pre> <p>The SSL files will be read and the Console will configure correctly.</p>
ESM-34568	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <pre>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</pre> <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>
ESM-31433	<p>The following exception might appear in the Manager's log file:</p> <pre>ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open</pre> <p>Workaround: This error is not serious. It is automatically resolved within one week of the Manager startup during which time the Manager rebuilds the resource search index (done weekly). You may choose to ignore the error, or manually do a rebuild at any time by running the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create -m &lt;manager-hostname&gt; -u &lt;admin-user-name&gt; -p &lt;password&gt;</pre>
ESM-30670	<p>If the search index file becomes corrupted, the search index will be out-of-date and the following message appears in the Manager's log file:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Re-generate the index by issuing the following command from the Manager's bin directory:</p> <pre>arcsight searchindex -a create -m &lt;manager-hostname&gt; -u &lt;admin-user- name&gt; -p &lt;password&gt;</pre>

## ArcSight Web

Issue	Description
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>

## Installation and Upgrade

Issue	Description
ESM-51846	<p>During installation of ESM 5.6 on non English Windows 2012 R2 server, the installer pops up a warning message:</p> <p>"You are installing this product on a unsupported platform."</p> <p>You can ignore this message.</p>
ESM-51700	<p>On uninstallation of ESM 5.6, the uninstaller displays a warning message "All items could not be removed", however all files are actually removed. This message can be safely ignored.</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.</p> <p>Workaround: Use following commands to create the dump file:</p> <pre>cd %ARCSIGHT_HOME%\bin open the file named system.param remove the two lines that starts with old and new like below. old 1: select table_name    ',' from user_tables where tablespace_name='ARC_SYSTEM_DATA' and table_name &lt;&gt; 'PLAN_TABLE' &amp;1 '&amp;2' new 1: select table_name    ',' from user_tables where tablespace_name='ARC_SYSTEM_DATA' and table_name &lt;&gt; 'PLAN_TABLE' and upper(table_name) not like 'ARC_SLD_%' Save the file. cd &lt;ARCSIGHT_HOME&gt;\bin expdp &lt;username/password@instance&gt; directory=ARCSIGHT_DUMP_DIR dumpfile=arcsight.dmp parfile=&lt;ARCSIGHT_HOME&gt;\system.param</pre>
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>