

Release Notes ArcSight™ ESM

Version 5.2

March 2012



Release Notes ArcSight™ ESM Version 5.2

Copyright © 2012 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.arcsight.com/copyrightnotice>

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
04/06/2012	ArcSight™ ESM Version 5.2	Added ESM-49830 and ESM-49827 to the "Open Issues in v5.2" section
03/09/2012	ArcSight™ ESM Version 5.2	Release Notes for ArcSight™ ESM Version 5.2

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

ArcSight ESM Version 5.2	5
Welcome to ArcSight ESM Version 5.2	5
What's New in This Release	5
Oracle Support	6
Upgrade Support	6
Geographical Information Update	6
Vulnerability Updates	6
Usage Notes	7
JRE on Macintosh	7
AIX 6.1 and Oracle PSU	7
Patch for Russia/Belarus DST Changes	7
Oracle Password Expiration Issue	7
Session Expiration in ArcSight Web	8
Browsers and Custom View Dashboards	8
Fixed Issues in v5.2	9
Analytics	9
ArcSight Console	9
ArcSight Database	10
ArcSight Manager	10
ArcSight Web	11
Installation and Upgrade	11
Localization	11
Pattern Discovery	11
Open Issues in v5.2	12
Analytics	12
ArcSight Console	14
ArcSight Database	18
ArcSight Manager	20
ArcSight Web	22
Connectors	23
Installation and Upgrade	23
Localization	25
Pattern Discovery	25

ArcSight ESM Version 5.2

Welcome to ArcSight ESM Version 5.2

ArcSight Enterprise Security Management (ESM) v5.2 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 v5.2 release.

Reporting

Reporting has been enhanced to create a report once and distribute it to multiple recipients. You have the option to not send empty reports. Reporting has also been enhanced to define non-ESM users as recipients.

Standard Content

Administration foundation: Made navigation of administration tasks easier by adding use cases and enhancing the resource monitoring content to better monitor query-based resources (reports, trends, and query viewers).

Correlation

New, light-weight rules that skip multiple event aliases and aggregation, limit actions and auditing for significant performance gains.

Active List Enhancements:

- SUM, MIN, MAX numeric subtypes
- Store data in time segments
- Enhanced variable functions to support active lists

Dashboards

Enhanced to support greater drill-down from data monitors and query viewers to dashboards, reports, active channels, and query viewers.

Asset Model Import Connector

The Asset Model Import Connector now supports the ability to create and manage the Asset Model within ESM. The Asset Model Import Connector monitors changes in an asset model CSV file, enabling you to manage and maintain your Asset model more easily.

Oracle Support

ESM v5.2 does not support Oracle 10.2.0.4. If you are using Oracle 10.2.0.4, you must upgrade your Oracle instance to 11.2.0.2. You can do so using the ESM v5.0 SP2 ArcSight Database installer. Refer to the ESM v5.0 SP2 Upgrade Guide for detailed instructions on upgrading the Oracle software.

If you are currently using Oracle 11.2.0.1, you must first upgrade your Oracle software to 11.2.0.2 by upgrading to ESM v5.0 SP2 patch2 before upgrading to v5.2. Refer to the ESM v5.0 SP2 Patch2 release notes for detailed instructions to do so.

Oracle PSU

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

Upgrade Support

The following upgrade paths are supported for this release:

- ESM v5.0 SP1 Patch 3 to v5.2
- ESM v5.0 SP2 Patch2 to v5.2

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



Caution

If you are upgrading from ESM 5.0 SP2 Patch 2 to ESM 5.2, you will not be able to benefit from some of the fixes available in ESM 5.0 SP2 Patch 2 after you upgrade to v5.2. ESM v5.2 does not include the fixes made in v5.0 SP2 Patch 2. However, you can get these fixes when ESM 5.2 Patch 1 becomes available. Please refer to the ESM 5.0 SP2 Patch 2 release notes to see the list of these fixes.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20120101.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU 563	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
Enterasys Dragon IDS	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S616	Bugtraq, CVE
Juniper / Netscreen IDP 2061	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
TippingPoint UnityOne DV8300	Faultline, Bugtraq, CVE, Nessus, MSSB
Fortinet Fortigate	Faultline, CVE, Nessus, MSSB
ISS SiteProtector	Faultline, Bugtraq, CVE, Nessus, X-Force, CERT, MSSB

Device	Vulnerability Updates
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, Nessus, MSSB, MSKB, CERT
McAfee HIPS 7.0	CVE
Radware DefensePro	CVE, MSSB

Usage Notes

ESM v5.2 introduces some improvements to existing features. There are a few things to consider when using these features. Please review the following points to ensure smooth operation.

JRE on Macintosh

On the Macintosh platform you will need to first install JRE 1.6.0_26 before installing ESM v5.2.

AIX 6.1 and Oracle PSU

After you apply the Oracle PSU on AIX 6.1, you will receive a dblink error. To resolve this issue you need to apply the AIX efix IV09580 patch. Please see <http://www.ibm.com/developerworks/forums/thread.jspa?messageID=14728034> for details on this issue.

Patch for Russia/Belarus DST Changes

If you use time zones in Russia or Belarus, ESM v5.2 includes updates to support Russia's and Belarus' transition away from Daylight Savings Time.

On Oracle 11.2.0.2

Oracle 11.2.0.2, however, requires that you apply the Oracle portion of the patch provided in the ESM Hot Fix RDST2011029 to support this time zone change. You can download its Readme file (which provides the instructions on installing the patch as well as post installation procedures) from the HP Software Support Online download site.

On SmartConnectors

If you are running SmartConnector version 5.1.6.6014 or earlier, you must apply Smart Connector Hot Fix RDST2011029 to your SmartConnectors, or upgrade to SmartConnector version 5.2.1.6186 or later. On SmartConnector releases starting from 5.2.1 onwards the DST issue has already been fixed, so you need not apply the Hotfix.

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 SSI, certificate will be used to login. For CAC or Radius the authentication dialog will open 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 you want.

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

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

Fixed Issues in v5.2

Analytics

Issue	Description
ESM-49438	The Use Cases configuration wizard shows empty pages for Introduction, Prerequisites and Summary. This is because the Use Case configuration wizard is not implemented for the ArcSight Administration use cases.
ESM-49371	The behavior of Active Channel, Query Viewer and Reports has been made consistent in regard to a missing user-enforced filter. The new behavior for any new custom user group that has neither an event filter nor an inherited event filter will be as if the filter was No Events.
ESM-47496	The Connector Monitoring report was using the Connector ID (the connector's resource ID), because of which the report would show the caching history of only one connector at a time. The query condition has been changed to use the Connector URI instead of the Connector ID, and uses StartsWith instead of =, so that groups of connectors, or a single connector, can be in the report.
ESM-46828	<p>The rules engine recovery process did not properly restore the state of rules with an aggregation threshold greater than 1. For example, a rule looks for 10 events matching certain conditions with an OnFirstThreshold trigger. If five matching events were received prior to a Manager restart, and five more were received after the restart, the threshold trigger would not fire because the partial aggregation state was not reset correctly during recovery.</p> <p>The problem did not affect join rules. For a rule with multiple event aliases, if a subset of the event aliases were matched prior to restart and the remaining ones were matched afterward, the rule would fire correctly. This has now been fixed.</p>

ArcSight Console

Issue	Description
ESM-49052	Filters having conditions on Conditional variables, which return Actor list field, could not be used in Queries and ActiveChannels. These filters could only be used in Rules and DataMonitors. It affected content developers using Conditional Variables in ESM. This issue has now been fixed.
ESM-47824	<p>Prior to this release, a trend built on a query that contained multi-mapped active list fields or overlapped session list fields via a global variable would show the following problems:</p> <ul style="list-style-type: none"> - If the query contained a list field of Timestamp type, the trend would fail to be viewed in the Console. - Condition editor in the Console would not show proper operators on the fields list for a query on the trend. <p>This issue has been fixed in v5.2.</p>
ESM-46633	The Help window for Rules was inactive. This was seen while defining a Set Event Field action. This issue has now been fixed.
ESM-46632	On the Rule Editor's Aggregation Tab, if you selected the Add button and then clicked Help, it opened the wrong help topic. This has been fixed in this release.
ESM-40943 TTP#67697	On the normal layout, Status text labels next to the icons are visible. On the custom layout, Status text labels were sometimes not displayed. This was an intermittent problem that was seen on the embedded browser and would go away once the data monitor was refreshed. This issue has now been fixed.

Issue	Description
ESM-40506 TTP#66753	<p>On the Macintosh platform, setting Safari as the preferred external browser using the Console's Preference menu (Edit>Preferences>Program) would result in the wrong URL.</p> <p>The workaround was to change the setting in the Console's Preference menu (Edit > Preferences > Program > Preferred Web Browser > External Browser) to set a default external browser to be Safari. In Mac OS, set Safari as the default browser (Safari > Preference > General > Default).</p> <p>This issue has now been fixed.</p>
ESM-39322 TTP#64233	<p>When viewing a Category Model, if the user was a non-admin user, a NullPointerException was thrown by the Arcsight Console, even if the user had been given read and write rights on all the actors and the Actor Base field set. The workaround was to view the Category Model as an admin user. This issue has now been fixed.</p>
ESM-39101 TTP#63834	<p>In Suite B mode, the custom view dashboard could not be launched. The workaround was to use an external web browser. This issue has now been resolved.</p>
ESM-38415 TTP#62565	<p>In an active channel, you could not add global variables to the channel through the right-click option, Add Column. Only global variables already added to the current field set would be displayed. This is no longer an issue. With this release, you cannot add Variables directly to channel. The 'Variables' menu option is available only when a fieldset associated with a channel has variables. Otherwise, the 'Variables' option does not show up.</p>
ESM-36034 TTP#56996	<p>The On Time Unit (OTU) evaluation in Rule Actions triggered correctly as long as matching events continued to occur, but the rule chain for the OTU alert only included events from the previous minute. Triggering with time periods longer than a minute did not work correctly. For example, if OTU was set to trigger every 3 minutes, the OTU alert included base events from the previous minute and not from previous 3 minutes. This issue has now been fixed and the "On Time unit" value is taken into effect for rule action.</p>

ArcSight Database

Issue	Description
ESM-46330	<p>The command line function to archive, deactivate, or reactivate partitions did not work if non-default values of archive, retention, and reserve period days were used. This has now been fixed.</p>

ArcSight Manager

Issue	Description
ESM-30307 TTP#42710	<p>The rule editor did not allow more than 999 matches on the rules aggregation tab. Any value greater than 999 matches were reset to 999. To work around this, you had to specify the following property in console.properties file:</p> <p>console.rule.max.threshold=####.</p>

ArcSight Web

Issue	Description
ESM-48712	Drilldown was disabled for query viewer fields when its related query was NOT on Event. This issue has now been fixed.
ESM-38676 TTP#63013	On ArcSight Web, inline filtering was not supported for local or global variables. With this fix, you can create an inline filter condition on a variable the same way as you did on a regular field.

Installation and Upgrade

Issue	Description
ESM-45566	If your ESM was installed in FIPS mode, when upgrading the Console, the Console configuration wizard didn't maintain the previous configuration. The Console configuration wizard displayed the default authentication as "Password Based" instead of what was set in the original Console configuration. This has now been fixed.

Localization

Issue	Description
ESM-46567	In a localized environment, the Group variable functions, for example GetGroupsOfAsset and FormatGroupsOfAsset, did not return results in Active Channels. This has now been fixed.

Pattern Discovery

Issue	Description
ESM-46312	If you created a rule from patterns that use domains, you had to aggregate the field, Domain Name. If this field was not aggregated, the rule would not get triggered. This has now been fixed.
ESM-46250	If a domain field is shared by more than one domain, the event graph was not displayed correctly. This has now been fixed.
ESM-46157	In the Profile Actions tab, Global Variables were unavailable for Add to Active List and Add to Session List actions. For example, when Add to Active List was selected for On Pattern Discovered action, the Active List and the Active List field mappings needed to be provided. In the drop-down menu of the field mapping, the Global Variables were disabled. This issue has been fixed in this release.

Open Issues in v5.2

Analytics

Issue	Description
ESM-49768	The ESM Installation Guide lists the MAC OS installer as ArcSight-5.2.x.nnnn.y-Console-MacOSX.bin, however, it should be ArcSight-5.2.x.nnnn.y-Console-MacOSX.zip.
ESM-49766	The ESM Installation Guide and User Guide make reference to Solaris as a supported platform for the ESM Console. As of ESM 5.2, Solaris is no longer a supported platform for the ESM Console. For details of ESM's product life cycle support, see the ESM 5.2 Product Life Cycle document posted to Protect 724.
ESM-49436	Filters having conditions on Conditional Variables which return Actor list field, cannot be used in Queries and ActiveChannels. These filters can only be used in Rules and DataMonitors. It affects content developers using Conditional Variables in ESM.
ESM-49187	The Text (Column Names/Field Names/Aliases) in the Table Header will not be able to 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 firing. A single rule can correlate such audit events, but any subsequent chaining rules will be suppressed.
ESM-48537	If a rule contains multiple negated event aliases with timeout values specified, the rule will not fire 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 will not fire 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 will not fire at all because event1 will be removed from memory prior to the cumulative timeout. Workaround: We recommend that you specify a positive timeout value for only one negated alias, and set the remaining timeouts to zero.
ESM-47918	There is an intermittent issue where TRM does not return an appropriate response when an update to Quarantine Node by IP command is sent.
ESM-46219	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. 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.
ESM-40795 TTP#67303	Custom cell names created in ArcSight ESM v4.x are not validated for name conflicts with global and local variable names in this release. If you experience issues due to name conflicts, change your custom cell names.

Issue	Description
ESM-40529 TTP#66801	<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-40449 TTP#66622	<p>When exporting events from the Case Details channel, archived events do not get exported.</p>
ESM-39632 TTP#64943	<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 TTP#63460	<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-38079 TTP#62044	<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>
ESM-37810 TTP#61524	<p>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.</p>
ESM-35381 TTP#55314	<p>Variable names that contain hyphens (-) do not work properly when included on the right side of a comparison in a condition statement. For example, consider a rule with a condition that compares the JME argument sqrt(4) to a variable named abc-cde, where the value of abc-cde is:</p> <p>add (2.0,3.0)</p> <p>This rule will not trigger successfully, and the logs will show an exception indicating ESM is "unable to evaluate rule."</p> <p>Workaround: Do not use hyphens (-) in variable names. Preferably use upper and lower case letters only, although you can use underscores (_) too.</p>
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-34872 TTP#53975	<p>You cannot send pager notifications through the pager service provider.</p> <p>Workaround: If the pager supports receiving e-mails, create notification destinations in the Console by providing the e-mail address of the pager in the e-mail destination.</p>
ESM-34531 TTP#53435	<p>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.</p>

Issue	Description
ESM-33525 TTP#51280	<p>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>The query run failed because of the following reason:</p> <p>com.arcsight.common.ArcSightException: com.arcsight.common.introspection.queryable.QueryableFetchException:</p> <p>Encountered persistence problem while fetching data: Unable to execute query: ORA-00979: not a GROUP BY expression</p> <p>Conditional variables in a SELECT statement with an aggregated field causes an Oracle exception (not a GROUP BY expression)</p> <p>Workaround:</p> <ol 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 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 saving it. This will force the re-validation of the trend and re-enable the trend.</p>
ESM-29348 TTP#39407	<p>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>

ArcSight Console

Issue	Description
ESM-49827	When upgrading to ESM v5.2 from previous versions, drill-downs for user-created query viewers are not migrated to the upgraded system.
ESM-49289	<p>In localized environments, query viewers don't open from data-monitor drill-downs.</p> <p>Workaround: Manually launch the respective query viewer.</p>
ESM-49270	<p>In the Custom Layout of a dashboard, if you try to change the display format of a data monitor, say from "Bar Chart" to "Table" and you save the dashboard. The next time that you reload the dashboard, the data monitor will still display in the "Table" format. The display format can not be changed in the Custom Layout.</p> <p>Workaround: Change the display format in other layouts.</p>
ESM-48908	When viewing custom layout dashboards in an external browser, the Show Events menu option will not launch the Event Inspector.

Issue	Description
ESM-48207	The context menu for Query Viewers in Image Dashboard is specific to Data monitors and may not work.
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 having been 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-41344 TTP#68478	<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 TTP#68262	<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-41116 TTP#68018	After creating a statistics data monitor, adding it to the dashboard, and switching to custom view mode, the dashboard does not get launched. This happens on the external Internet Explorer (IE) browser on a 64-bit Windows platform. This is because Adobe Flash Player is required but is not supported on IE on 64-bit systems.
ESM-41019 TTP#67856	<p>When you have client-side authentication set up, if the Manager is configured with the "Password and SSL 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 ArcSight ESM Administrator's Guide for details on how to do this.</p>

Issue	Description
ESM-40935 TTP#67689	On a Windows Vista 64-bit system, charts cannot be viewed in custom view dashboards when using Internet Explorer (IE) as the external browser. Workaround: Use the 32-bit browser, such as 32-bit version of IE or Mozilla Firefox, and also download Adobe Flash Player.
ESM-40917 TTP#67652	If you delete a large number of actors through the ESM Console, the Console may become temporarily unusable. However, the Manager will continue processing in the background and will update the database with your changes. Once the Console becomes available again, deletion from the database may take longer. In some cases, for instance if the server is terminated or encounters an error, not all deletions may be completed, leaving the actors data in an inconsistent state. Contact Customer Support for assistance in detecting and cleaning up this condition if you suspect it has occurred.
ESM-40739 TTP#67195	The very first time that you start the Console, you must restart the Console after accepting the Manager's certificate in the popup. This is required in order for the Custom View dashboards to work properly.
ESM-40587 TTP#66906	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. 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.
ESM-40302 TTP#66337	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.
ESM-39980 TTP#65708	The Console can become unresponsive if you access other resources while building category models with a large number of actors.
ESM-39963 TTP#65671	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. Workaround: There is no workaround at this time. Ignore the duplicate rows.
ESM-39856 TTP#65477	If you use the embedded browser in Windows to view a report, the report may not appear until you resize the panel. Workaround: Resize the panel before running a report. You may want to try several resizings to get the desired results.
ESM-39829 TTP#65421	When there are category models in ESM, deleting actors will require these category models to be re-built. Each rebuild may take seconds. In case thousands of actors are deleted, the whole deletion period may last for hours because actor deletion launches a category model rebuild.
ESM-39331 TTP#64251	If you create an Actor channel, add any new fields to the field set being used by the channel instead of 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-38014 TTP#61931	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. Workaround: Manually set the filter for such data monitors that are identified by the broken resource icon.

Issue	Description
ESM-37868 TTP#61659	<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 TTP#60500	<p>On a 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: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.</p>
ESM-36055 TTP#57050	<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, 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.</p>
ESM-35998 TTP#56865	<p>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.</p>
ESM-35830 TTP#56367	<p>ESM v5.2 is compatible with TRM v4.6. However, certain commands that were introduced in a later version of TRM are available when you use the integration tool from TRM v4.7 to connect to TRM v4.6. If you try to execute such commands, you will receive a java.lang.NullPointerException exception. One such command introduced in TRM v4.7 is Generate N/W detail as CEF.</p> <p>Workaround: We recommend that you upgrade to TRM v4.7 or higher. If you upgrade to TRM v5.0, you will be able to use the integration commands feature.</p>
ESM-35465 TTP#55476	<p>If you open 10 channels and view them, then delete these 10 channels from the resource tree, you will not be able to open any more channels. You will see the following error: "Unable to create communication mode with server:</p> <p>The maximum number of open event channels (10) has been exceeded. Please close one or more individual event channels to continue."</p> <p>Workaround: Restart the Console.</p>
ESM-34830 TTP#53912	<p>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.</p> <p>Note: Select a Connector in the Navigator, right-click and choose "Configure" to bring up the configuration for that connector in the Inspector panel. Select the "Default" tab and then "Content" subtab. The "Limit event processing rate" option is under "Processing." Only integer settings are supported for this option on the Console.</p>
ESM-33453 TTP#51094	<p>On Unix systems: The drag-and-drop feature does not work on the Console.</p> <p>Workaround: Use the cut-and-paste feature instead.</p>
ESM-33440 TTP#51072	<p>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.</p>
ESM-33360 TTP#50968	<p>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.</p>
ESM-32705 TTP#49608	<p>In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range.</p> <p>Workaround: Delete the existing color mapping and create a new one with the color mapping of your choice.</p>

Issue	Description
ESM-32489 TTP#49024	Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.
ESM-30791 TTP#44028	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-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.
ESM-26488 TTP#33835	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-49730	On a Linux 64-bit machine, you could see the following error when trying to enable and disable FIPS mode on ArcSight Web, the Partition Archiver, and ArcSight Console: <pre>./arcsight runmodutil -fips false -dbdir /opt/arcsight/db/user/agent/nssdb.client/ Assuming ARCSIGHT_HOME: /opt/arcsight/db Assuming JAVA_HOME: /opt/arcsight/db/jre ArcSight modutil starting... /opt/arcsight/db/bin/nss/linux/modutil: error while loading shared libraries: libz.so.1: cannot open shared object file: No such file or directory.</pre> Workaround: Install the 32 bit zlib package on your machine.

Issue	Description
ESM-48270	<p data-bbox="493 260 1365 321">There is a performance issue when running channels or queries with conditions on actor global variables.</p> <p data-bbox="493 333 1328 384">Workaround: If you are experiencing this problem, the following tips might be helpful in improving performance.</p> <ol data-bbox="493 396 964 420" style="list-style-type: none"> 1. Generate session list statistics as follows: <p data-bbox="493 434 1284 485">Run the following three commands in <ARCSIGHT_HOME>\bin on your database machine:</p> <pre data-bbox="524 497 1224 594">./arcdbutil sql username/password @../utilities/database/oracle/common/sql/runSessionListStats.sql exec runSessionStats</pre> <p data-bbox="493 609 1360 684">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 data-bbox="493 699 1365 722">Note that the scripts may run for a long time if the session lists have a lot of data.</p> <ol data-bbox="493 737 1360 993" style="list-style-type: none"> 2. You could also reduce the rownum limit from default value 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 (the way to run is specified in the Query and Trend Performance Tuning section) will also help to improve the overall read performance of the system. This may take between few minutes to few hours depending on the volume of events. 4. Also, eliminating the LIKE condition from the query will extensively improve the query performance.
ESM-48248	<p data-bbox="493 1018 1360 1094">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 data-bbox="493 1108 630 1129">Workaround:</p> <ol data-bbox="493 1144 1300 1278" style="list-style-type: none"> 1. Log in to Oracle as "sysdba". 2. Run the following SQL command from the sqlplus prompt: <pre data-bbox="524 1218 1300 1241">alter system set "_optimizer_distinct_agg_transform"=false scope=both;</pre> 3. Restart Oracle to apply the change to all sessions.
ESM-46556	<p data-bbox="493 1304 1360 1379">During the Oracle database installation, when you create a database instance, the wizard does not warn you if you use an instance name with a space (for example, arcsight db).</p> <p data-bbox="493 1394 1360 1444">Oracle does not allow spaces, and therefore the instance creation will fail if the instance name has a space in it. Do not use spaces for database instance names.</p>
ESM-35884 TTP#56521	<p data-bbox="493 1470 1360 1520">If you start the Partition Archiver as a service, the PATH does not get set correctly for the Oracle user if you use /usr/bin/bash.</p> <p data-bbox="493 1535 630 1556">Workaround:</p> <ul data-bbox="493 1570 1333 1692" style="list-style-type: none"> - While logged in as the oracle user, run the Partition Archiver as a standalone application with "arcsight agents" command. or - Switch to /bin/sh which is the default Oracle shell in /etc/passwd.

Issue	Description
ESM-35620 TTP#55853	<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 TTP#53484	<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-49830	<p>In a hierarchical ESM deployment where you have source Managers and destination Managers, the destination Manager will occasionally misidentify the forwarded event when the event is forwarded from source to destination. This will result in an Event ID that could be a duplicate of an existing event in the database on the destination Manager, or result in an Event ID that will soon be a duplicate of a future Event ID.</p> <p>In either case, the end result will be local and remote events with duplicate Event IDs. This might impact the retrieval of base events from the source Manager.</p>
ESM-49745	<p>After a scheduled rule task has completed, an exception (NullPointerException) is printed to the manager server.std.log file, and the replay directory (rules/batched/checkpoint) is not cleaned up after the run. The error is relatively harmless; however, after a restart, the Manager may rerun the previous scheduled rule group.</p> <p>Workaround: Delete the mentioned directory manually prior to restart.</p>
ESM-49733	<p>On Solaris 11, the service command "arcsight_manager stop" to stop the Manager's service does not work.</p> <p>Workaround: Run the alternative command "arcsight managerstop" from the Manager's <ARCSIGHT_HOME>/bin directory to stop the Manager.</p>
ESM-48784	<p>If a customer name contains the special character '&' in the OI (organization group(s)) the group does not get processed when translated to a URI. When this happens, it prevents any Actor from getting created in the List.</p>
ESM-41331 TTP#68451	<p>After the resource validation process is run, assets that are actually invalid appear to be valid.</p> <p>Workaround: Manually mark assets that are known to be invalid as invalid.</p>
ESM-41215 TTP#68187	<p>On SUSE 11, the ESM Manager does not start automatically at system startup even if this option was selected during installation.</p> <p>Workaround: Start the Manager manually.</p>

Issue	Description
ESM-41168 TTP#68098	Uninstalling and then re-installing the global variable package causes an exception. Global variables are part of the core content and uninstalling core content is not recommended.
ESM-40889 TTP#67567	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.
ESM-40866 TTP#67496	<p>Importing packages or archives containing assets in zones that were modified will cause those assets to become invalid. This happens if you are importing archives from older releases.</p> <p>Workaround: Post import, you need to manually fix the zone for these assets.</p>
ESM-37633 TTP#61154	<p>After installing the Manager, you will see an error in the server.log file:</p> <p>[ERROR][default.com.arcsight.config.util.WebProperties][getPassword]</p> <p>com.arcsight.common.ArcSightException: Cannot handle the data which was obfuscated by old scheme</p> <p>This message is harmless and can be safely ignored.</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	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.
ESM-33431 TTP#51053	<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>
ESM-31433 TTP#46276	<p>You may see the following exception in the Manager's log:</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>

Issue	Description
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:</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>
ESM-30008 TTP#41582	<p>Occasionally, when installing an exported package from a bundle file, you might receive the following error:</p> <pre>Install Failed: Resource in broker is newer than modified resource.</pre> <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>
ESM-27414 TTP#35166	<p>When running the Send Logs wizard If you click Previous or Next, you might get an error that says:</p> <pre>Error (Null).</pre> <p>Workaround: Cancel the wizard and start again.</p>

ArcSight Web

Issue	Description
ESM-49668	<p>On AIX, reports will fail to run from ArcSight Web. However, you will be able to run reports on the Console.</p>
ESM-35801 TTP#56258	<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 TTP#56005	<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>

Issue	Description
ESM-33922 TTP#52336	<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 virtually unreadable.</p> <p>On the ESM 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 ESM 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 ESM 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	<p>Due to a limitation in Adobe Flash Player, to view dashboards within ArcSight Web on a 64-bit operating system, you are required to 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>

Connectors

Issue	Description
ESM-41419 TTP#68697	<p>If a connector needs to send events to multiple ESM Manager destinations with different versions (for example, v4.5 and v5.0), the serialization framework uses the lowest common denominator version (v4.5 in this example) to serialize events prior to sending them to the ESM Managers. So, only v4.5 events will be sent to both ESM Managers.</p>

Installation and Upgrade

Issue	Description
ESM-49704	<p>The ESM Installation Guide lists the incorrect versions of the supported MAC OS for the ArcSight Console. The correct versions should be 10.6 and 10.7, as indicated in the PLD that supports this release.</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-48833	<p>During the Manager upgrade, you might see the following error message in the upgrade logs. You can safely ignore this error message as this is transient and does not impact any functionality.</p> <p>[ERROR][default.com.arcsight.common.introspection.dependentvariable.DependentVariableIntrospector][_addSubDependentVariables] Data List schema not available for function field : get_activelist_value</p>
ESM-46545	<p>After upgrade, the number of invalid assets listed in the Resource Validation Report may be higher than before the upgrade. This is due to additional validations introduced in ESM v5.0 SP1 release to identify invalid assets.</p>
ESM-41148 TTP#68075	<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 TTP#67797	<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 TTP#55935	<p>ESM Console upgrades from 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> <pre>arcsight consolesetup</pre> <p>The SSL files will be read and the Console will configure correctly.</p>
ESM-35599 TTP#55810	<p>When upgrading the ArcSight Console, you will be prompted to enter the path to the previous Console installation. Be sure to provide the path to the Console's <ARCSIGHT_HOME>/current directory of your previous Console installation.</p> <p>If you do not point to the "current" directory, you will get an error that the cacerts folder could not be found in this location. Selecting OK will allow you to continue with the upgrade. But, this will cause the certificates to not get transferred and make the upgrade error prone.</p>
ESM-34891 TTP#54003	<p>This release does not support spaces in install paths for the ArcSight Database, ESM Manager, ArcSight Console or ArcSight Web server. If there are spaces in the install paths, ESM Database, Manager, ArcSight Console and ArcSight Web setup wizards might not work, and ESM Manager startup will generate exceptions. This is an issue on all platforms.</p> <p>Workaround: Do not use spaces in ESM installation paths. The default install paths (e.g., C:/arcsight/Manager) do not include spaces. If you modify the install paths, just make sure there are no spaces in the directory names. Dashes (-) or underscores (_) can be used instead of spaces.</p>

Issue	Description
ESM-33949 TTP#52394	<p>File resources are not handled properly during ESM upgrades. This results in unassigned file resources after the upgrade. For example, .art files are created as new file resources and get new version IDs during the upgrade. The original files are stored in the Files resource under the Unassigned folder.</p> <p>Workaround: You can remove the unassigned .art files after an upgrade, since they are duplicates. The .art files can be safely deleted.</p>
ESM-31766 TTP#47206	<p>During a Manager upgrade, the "SSL Client Only" authentication option is selected by default. Even if you had set up your existing Manager to use the "Password Based and SSL Client Based Authentication" method, the authentication method selected in the upgrade wizard panel will still default to "SSL Client Only".</p> <p>Workaround: Make sure to change the authentication method back to "Password Based and SSL Client Based Authentication".</p>
ESM-31392 TTP#46153	<p>On Solaris: When performing a fresh ESM Manager installation or upgrading ESM, the installation or upgrade does not always complete when solutions packages are installed.</p> <p>Workaround: Check the system requirements for your Solaris system in the "Supported Platforms" section of the "Installing ArcSight Manager" chapter in the ESM Installation and Configuration Guide to ensure that your system meets the minimum requirements.</p>

Localization

Issue	Description
ESM-49740	<p>For non-English locale environment, only English characters are supported for user name and password. Using non-English characters for user name and password might result in authentication issues.</p>

Pattern Discovery

Issue	Description
ESM-35048 TTP#54452	<p>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.</p>

