

# **Release Notes ArcSight™ ESM**

---

Version 5.0 SP1

January 6, 2011



## Release Notes ArcSight™ ESM , Version 5.0 SP1

Copyright © 2011 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:  
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

### Revision History

Date	Product Version	Description
1/6/11	ArcSight™ ESM Version 5.0 SP1	Release Notes for ArcSight™ ESM Version 5.0 SP1

### ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	<a href="mailto:support@arcsight.com">support@arcsight.com</a>
Support Web Site	<a href="https://support.arcsight.com">https://support.arcsight.com</a>
Customer Forum	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

# Contents

---

<b>ArcSight ESM Version 5.0 SP1 .....</b>	<b>1</b>
Welcome to ArcSight ESM Version 5.0 SP1 .....	1
What's New in This Release .....	1
ArcSight Oracle 11g Release 2 Database Platform Support .....	1
Pattern Discovery Enhancement .....	1
Correlation Enhancements .....	1
Section 508 Enhancements .....	1
Localization Support .....	2
New Platform Coverage .....	2
Upgrade Support .....	2
Geographical Information Update .....	2
Vulnerability Updates .....	2
Usage Notes .....	3
Embedded and External Browsers .....	3
Getting an Error Message During an Upgrade .....	4
Configuring Shared Memory on Linux .....	4
Avoiding DB Write Performance Issues with Oracle 11g .....	6
Documentation-Related Notes .....	6
Open Issues in v5.0 SP1 .....	8
Analytics .....	9
ArcSight Console .....	13
ArcSight Database .....	18
ArcSight Manager .....	20
ArcSight Web .....	24
Connectors .....	24
Installation and Upgrade .....	25
Localization .....	28
Pattern Discovery .....	28
Issues Fixed in ESM 5.0 SP1 .....	29
Analytics .....	30
ArcSight Console .....	32
ArcSight Database .....	34
ArcSight Manager .....	34
ArcSight Web .....	36

Installation and Upgrade .....	36
--------------------------------	----

# ArcSight ESM Version 5.0 SP1

---

## Welcome to ArcSight ESM Version 5.0 SP1

ArcSight Enterprise Security Management (ESM) v5.0 SP1 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 v5.0 Service Pack 1 release. This section only highlights some of the major improvements in this release; you should reference the "Whats New" topic in the product online help for complete details.

### ArcSight Oracle 11g Release 2 Database Platform Support

ArcSight ESM v5.0 SP1 introduces support for Oracle 11g Release 2 as the primary version for new installations and also support for upgrading from existing Oracle 10G on Windows and Linux platforms.

### Pattern Discovery Enhancement

As part of ESM v5.0 SP1, Pattern Discovery introduces support for local and global variables as well as domain fields.

### Correlation Enhancements

Below is a high level summary of analytic enhancements introduced as part of the ESM v5.0 SP1 release:

- Variable support within list-based rule actions
- InActiveList condition support for actors
- Ability to aggregate on date fields in the rule conditions
- Report charts have been enhanced to support speedometer type
- Data monitors have been improved to provide totals for alarms shown

### Section 508 Enhancements

ArcSight Web now provides a warning when an active session is about to time out and provides the option to continue the session.

## Localization Support

ArcSight ESM v5.0 SP1 provides updated localization support for Japanese, Traditional Chinese and French languages based on the ESM v5.0 feature set.

## New Platform Coverage

Please review the ArcSight ESM v5.0 Platform Product Lifecycle document for details on OS platform support for the Manager, Database, Console, and ArcSight Web components. Here are some highlights concerning newly added platform support:

- **Red Hat Enterprise Linux 5.5 (RHEL 5)**

ArcSight ESM v5.0 SP1 Manager, Database and ArcSight Web introduces platform support for Red Hat Enterprise Linux 5.5(RHEL 5).

- **Microsoft Windows Server 2008 R2**

ArcSight ESM v5.0 SP1 Manager, Database and ArcSight Web introduces platform support for Microsoft Windows Server 2008 R2.

- **Microsoft Windows 7**

ArcSight ESM v5.0 SP1 Console has been enhanced to introduce platform support for Windows 7 64-bit.

- **Macintosh OS X v10.6**

ArcSight ESM v5.0 SP1 Console has been enhanced to introduce platform support for OS X v10.6.

## Upgrade Support

The following upgrade paths are supported for this release:

- ESM v5.0 to v5.0 SP1
- ESM v5.0 Patch 1 to v5.0 SP1

Please refer to the respective 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\_20101101.

## Vulnerability Updates

This release includes recent vulnerability mappings (November 2010 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 388	Faultline, Bugtraq, CVE, Nessus, MSSB
Enterasys Dragon IDS	Faultline, CVE, MSSB
Cisco Secure IDS S529	Faultline, Bugtraq, CVE, Nessus
McAfee Intrushield	Faultline, CVE
TippingPoint UnityOne DV8131	Faultline, Bugtraq, CVE, MSSB

Device	Vulnerability Updates
Fortinet Fortigate	Bugtraq, MSSB
ISS SiteProtector	CVE
Symantec Endpoint Protection	Faultline, Bugtraq, CVE
McAfee HIPS 7.0	Faultline, CVE
Radware DefensePro	CVE

## Usage Notes

ESM v5.0 SP1 introduces some new features as well as enhancements to some existing features. There are a few things to consider when using these features. Please review the following points to ensure smooth operation.

## Embedded and External Browsers

The Console's embedded browser is not supported on the following platforms:

- Red Hat Linux 5
- 64-bit Macintosh
- 64-bit Windows

On 64-bit platforms, use the 32-bit version of the browser. This limitation is due to lack of Adobe Flash Player support on 64-bit systems. Consider using an external browser instead, and use the 32-bit version of the browser. You select the browser at installation time or change it in your Console's Preferences menu.

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>

## 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>

## Scheduled Tasks

If the trigger time for a particular scheduled task run happens to fall during the transition time from daylight savings time (DST) to standard time (ST) or vice versa, the interval for that particular run will not be the expected interval.

Time zones that honor DST have a period of time that occurs twice during the transition from DST to ST. For example, in the US when changing from DST to ST, this hour occurs once while the DST is still in effect and again after switching to the Standard Time. The transition period occurs at 2 am, therefore 1:00:00 am - 1:59:59 am occurs twice (1:00:00 am PDT - 1:59:59 am PDT and 1:00:00 am PST - 1:59:59 am PST), where 1:00 am PST is 60 minutes after 1:00 am PDT. In this example, if the scheduled task is due to trigger any time between 1:00:00 am - 1:59:59 am, the interval for that particular run of the scheduled task will not be as expected.

Similarly, when the time changes from ST to DST, the 1:00:00 am - 1:59:59 am hour does not occur at all. The local time changes directly from 12:00 am to 2:00 am. So, if your scheduled task run was scheduled to trigger between 1:00:00 am - 1:59:59 am, the interval for that particular run will be off by an hour.

The interval calculation for subsequent scheduled runs do not get affected.

Currently, there are four time zones that are not supported in ESM:

- Kwajalein
- Pacific/Kwajalein
- Pacific/Enderbury
- Pacific/Kiritimati

These time zones fall in two countries, Marshall Islands and Kiribati.

## Getting an Error Message During an Upgrade

During an upgrade, you might get an error message similar to the following:

Could not create new group for URI filling: Group *<name of the group>* already contains a node with the same name as resource with id *<resource ID>*.

It probably means that you have a group in your pre-upgraded system that has the same name and URI as a system resource. To solve this problem, rename that group in your pre-upgraded system and try the upgrade step again.

## Configuring Shared Memory on Linux

Before creating the database instance on a Linux fresh install system, make sure you have enough shared memory on [/dev/shm](#) for the template you are planning to choose. This verification step is required because there is a possibility that you may not have the right amount of shared memory; and if you proceed with database instance creation with inadequate shared memory, the Oracle database memory parameters will not be set correctly.

To identify the available amount of shared memory on your system, check the size of [/dev/shm](#) from the Unix prompt by executing:

**df -k**

If shared memory is less than what you need, increase as required for your template creation using the following recommendations. Then proceed with the instance creation using the ArcSight Database software component.



The shared memory should be more than the following:

Template Size	Required Memory	Shared Memory Requirements
Small	246M	500M
Medium	740M	1G
Standard	1442M	3G
Large	2986M	4G
XLarge	6096M	7G
XXLarge	12160M	13G

After you complete the instance creation, do the following to verify if the instance was created with the correct parameters by running this command on the database machine.

**To verify parameters for the database instance:**

- 1 At the prompt, enter

**arcdbutil sql**

- 2 As user name, enter:

**/ as sysdba**

- 3 At the SQL prompt, enter:

**show parameter memory\_target**

The memory\_target value should be the same as the required memory specification in the above table for the chosen template. If it is correct, then you are done.

However, if memory\_target is set to zero, then do the following to correct the values.

**To verify SGA and PGA size if memory\_target is set to zero:**

- 1 Run the following command at the SQL prompt to check your SGA size and increase as required.

**alter system set sga\_max\_size=<Value\_from\_list\_below> scope=spfile;**

**alter system set sga\_target=<Value\_from\_list\_below> scope=spfile;**

**alter system set pga\_aggregate\_target=<Value\_from\_list\_below>  
scope=spfile;**

**shutdown immediate**

**startup**

**show parameter sga**

**show parameter pga\_aggregate\_target**

The values of the SGA and PGA should reflect the following values, depending on the chosen template.

Template Size	SGA_max_size/ SGA_target	PGA_aggregate_target
Small	182M	64M
Medium	538M	192M
Standard	1058M	384M
Large	2500M	512M
XLarge	6000M	1024M
XXLarge	11000M	4096M

- 2 At the prompt, enter **exit**.

## Avoiding DB Write Performance Issues with Oracle 11g

During fresh installations after creating the DB instance, you may need to modify the Oracle initialization parameter "[log\\_buffer](#)" in case you encounter problems with database write performance.

### To modify the `log_buffer` parameter:

- 1 At the prompt, enter  
**arcdbutil sql**
- 2 As user name, enter:  
**/ as sysdba**
- 3 At the SQL prompt, enter:  
**show parameter log\_buffer**  
The value will be set to a value around 1 MB.
- 4 Modify the `log_buffer` value to 14 MB:  
**alter system set log\_buffer=14237696 scope=spfile**
- 5 Shut down the Oracle instance for the changes to take effect. At the prompt, enter:  
**shutdown immediate**  
**startup**
- 6 To verify that the log buffer was reset correctly enter:  
**show parameter log\_buffer**  
The system should display **14237696**.
- 7 At the prompt, enter **exit**.

## Documentation-Related Notes

The following items were inadvertently left out of the ESM documentation and should be reviewed in addition to the ESM documentation.

## inActiveList Conditions for Queries

In a query, you can define an inActiveList condition and map multi-valued attributes to single-valued active list fields. For example, you have an active list that keeps track of roles, where one of the role values can be Normal, Restricted, and Privileged. You can test if an actor has one of these roles through the inActiveList condition. In this scenario, your list has a field called RoleName. You map the actor's role name attribute to this field. Keep in mind that an actor's RoleName attribute is multi-valued because an actor can have multiple roles. Through the inActiveList condition, your query will check if one of the actor's roles is, for example, Privileged.

## Viewing an Event or Resource Directly from Query Viewers

If you have event queries or resource queries, and they include an event ID or a resource ID field, you can go directly to that event or resource by right-clicking and selecting **View <Event> Details** or **View <Resource> Details**. For example, from a query viewer, you can drill down to:

- An event if the query includes the event ID field
- An actor if the query includes the actor ID field
- An asset if the query includes the asset ID field
- A case if the query includes the case ID field

## Open Issues in v5.0 SP1

The following issues are either new or carried forward from previous ESM releases and remain open in v5.0 SP1. These open technical issues merit your review to avoid difficulties. The following links will take you to issues you might encounter as you go through the workflow of installing, configuring, and using ArcSight ESM features:

- [“Installation and Upgrade” on page 25](#)
- [“ArcSight Manager” on page 20](#)
- [“ArcSight Database” on page 18](#)
- [“ArcSight Console” on page 13](#)
- [“Analytics” on page 9](#)
- [“Pattern Discovery” on page 28](#)
- [“ArcSight Web” on page 24](#)
- [“Localization” on page 28](#)
- [“Connectors” on page 24](#)

## Analytics

Issue	Description
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 v5.0 SP1. If you experience issues due to name conflicts, change your custom cell names.
ESM-40748 TTP#67210	After initially importing 50k Actors, you may experience sluggish performance in queries and channels. Performance improves after subsequent statistics collection.
ESM-40529 TTP#66801	After installing IdentityView 1.1, some previously valid ESM resources show as invalid resources.  Workaround: Edit the filter called Built In Identities on IDM System and remove the setAction local variable.
ESM-40449 TTP#66622	If you want to export events from the case details channel and there are archived events, the archived events will not be included in the export.
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: If this keeps happening, resize the panel before running a report. You may want to try several resizings to get the desired results.
ESM-39632 TTP#64943	Copying and pasting are not supported for conditions with variables. For example, if you create a filter for an active channel and used the Common Conditions Editor to add condition statements, copying and pasting into another editor (for example, a Rule editor) may result in an error.  Workaround: Manually re-enter the conditions.
ESM-39593 TTP#64837	There is a performance issue when running channels or queries with conditions on actor global variables.  Workaround: If you are experiencing this problem, then generate session list statistics as follows:  Run the following three commands in <ARCSIGHT_HOME>\bin on your database machine:  <pre>./arcdbutil sql username/password @../utilities/database/oracle/common/sql/runSessionListStats.sql exec runSessionStats</pre> 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. Note that the scripts may run for a long time if the session lists have a lot of data.
ESM-39554 TTP#64742	When querying events with conditions on actor fields, SQL queries may run slow especially in the following cases: <ul style="list-style-type: none"> <li>- List conditions are used.</li> <li>- Conditions on event fields are missing.</li> </ul> In some cases, queries may even time out and not produce results.
ESM-39371 TTP#64333	Query viewers and channels display list results differently. Query viewers display lists the way reports do: one line for each list entry while channels display lists the way data monitors do: [entry1, entry2, entry3].

Issue	Description
ESM-39044 TTP#63709	<p>IP addresses are not imported correctly into ArcSight Interactive Discovery (AID) from a CSV file. This is because the IP addresses are getting imported as floating point numbers and are therefore truncated. Importing from an Excel spreadsheet does not have this issue; however, the size limit of an XLS file prevents importing large data sets.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Create the CSV with the desired columns, for example: Name, Source Address, Destination Address.</li> <li>2. Create a schema.ini file that has the following definitions for the CSV file: <pre> [myfile.csv] ColNameHeader=True Format=CSVDelimited Col1="Name" Char Width 255 Col2="Source Address" Char Width 255 Col3="Destination Address" Char Width 255 </pre> </li> </ol> <p>This format instructs the driver that the IP addresses are to be imported as strings and not as numbers. The general format is as follows:</p> <pre> [myfile.csv] ColNameHeader=True Format=CSVDelimited Col1=A DateTime Col2=B Text Width 100 Col3=C Text Width 100 Col4=D Long Col5=E Double </pre> <p>For more information about the schema.ini file, perform an Internet search.</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: In the export and import, make sure to include the domain field set to which the domain fields belong.</p>
ESM-38702 TTP#63091	<p>When a group is added to a package, all its contents are automatically included. For top-level groups, as in the case of All Actors, this can include everything under this group. You can implicitly exclude an added group through the Only If Referenced option. This behavior applies to resources in general. If you create a package with a top-level group like All Actors, removing this package also removes all the resources of this top-level group's type.</p> <p>Workaround: To prevent accidental removal of a top-level group, as in the case of All Actors, create a group under it and add a number of actors to this group. Then add this group to a package. If you remove this package, you are only removing the associated groups and resources in that package.</p>
ESM-38079 TTP#62044	<p>If you rename a resource that has dependent resources, don't re-use the deleted 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>

Issue	Description
ESM-36755 TTP#58617	If you export an active list into a comma-separated values file and re-import from the same CSV file, the data is corrupted.
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: As a best practice, do not use hyphens (-) in variable names. Underscores (_) are acceptable in variable names, and upper and lower case letters only are best.</p>
ESM-35070 TTP#54507	<p>Verify Rules with Events (replay with rules) does not work for these types of active lists:</p> <ul style="list-style-type: none"> <li>- An event-based active list with values</li> <li>- A field-based active list with values, where all fields are mapped to event fields</li> </ul> <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>User is unable to set up sending pager notifications through the pager service provider.</p> <p>Workaround: If the pager supports receiving e-mails, create notification destinations in ArcSight Console by providing the e-mail address of the pager in the e-mail destination.</p>
ESM-34531 TTP#53435	When you set the Schedule Frequency for a report, the Next Run Time field is displayed incorrectly in the Editor. Even though the time is displayed incorrectly, the report runs at the time specified in the editor.
ESM-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.)</p> <p>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"> <li>1 Remove the ORDER BY fields in the Query resource.</li> <li>2 Use the sort options provided by the Query Viewer or the Report.</li> </ol>

Issue	Description
ESM-29633 TTP#40230	<p>Sometimes after changing a trend's description, another trend depending on this trend may become invalid. This affects all versions, all users, all ESM platforms.</p> <p>Workaround: You can usually re-enable a trend that was incorrectly disabled by making a minor change on the trend and then saving it. This will force the re-validation of the trend and usually re-enable the trend. For example, you could toggle the trend's enabled state off and then back on.</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 (e.g., one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (e.g., 24 hours if run once a day).</p>
ESM-26488 TTP#33835	<p>If you import the content of an older package into an existing newer package, the contents from the two packages get merged. The resulting package will consist of contents from both packages. The relationships will be merged, but the attributes will be picked up from the old package.</p> <p>Workaround: Export the new package to a bundle file so that you can recover it if need be. Then delete the new package before you import the old one.</p>



## ArcSight Console

Issue	Description
ESM-46633	The Help window for Rules is inactive. This is seen when you are defining a Set Event Field action. Click cancel or OK in the Set Event Field window. This will allow you to see the help information. After reading the help, you can go back to entering settings in Set Event Field.
ESM-46629	<p>On the Mac OS X with Safari as the default browser, the context Console Help is not displayed. Instead, the browser displays a blank Help page. This is a known Safari behavior, which does not accept more than one # character in the URL. The URLs to the Help pages contain more than one # symbol.</p> <p>Workarounds:</p> <p>Use either Firefox instead of Safari as the default browser. If you still want to use Safari, after the Help page loads, use the Contents tab to select the desired topic or use the Search tab to search for specific topics.</p>
ESM-46594	The Category Device Type field is not supported during event categorization from Console. You should not set the Category Device field.
ESM-46226	<p>The GetGroupOfAsset variable function does not return results in SQL mode (in conditions for reports, query viewers, pattern discovery, active channels). This problem is seen in all ESM platforms.</p> <p>There is no workaround at this time.</p>
ESM-46065	<p>The embedded browser is not supported in Solaris.</p> <p>Workaround: Use an external web browser to navigate help pages. Go to Preferences &gt; Global Options and check "Launch Help in external web browser"</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>This is a known issue. 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 cleartext in your browser URL parameters.</p>
ESM-41190 TTP#68141	If you set "LoggerPassword" as Password type and run Logger commands in the external browser, you will see an "Authorization Request" message in your browser.
ESM-41116 TTP#68018	After creating a statistics data monitor, adding it to the dashboard, and switching to custom view mode, the dashboard is not launched. This was seen using the external IE browser on a 64-bit Windows platform. This is because Adobe Flash Player is required but is not supported on IE in 64-bit systems.
ESM-41019 TTP#67856	<p>If Manager is configured with the "Password and SSL Authentication" and you have client-side authentication set up, 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 browsers and import the certificate into Manager's truststore; or 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-40999 TTP#67820	There is a performance issue when loading active channels. The channel starts to load but displays Loading Event ID for a few minutes before completely loading.
ESM-40985 TTP#67798	On Solaris only: From the Console, support for web browser functionalities is limited to only viewing the online help in the external browser.
ESM-40935 TTP#67689	On a Windows Vista 64-bit system, charts cannot be viewed in custom view dashboards when using IE as 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 are deleting a large number of actors through the Console, the Console may be temporarily unusable. ESM Manager continues processing in the background and updates the database with your changes. The Console becomes available again but 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 ArcSight support for assistance in detecting and cleaning up this condition if you suspect it has occurred.
ESM-40782 TTP#67265	The Console's embedded browser is not supported on Red Hat Linux 5. Workaround: Use the external browser instead.
ESM-40739 TTP#67195	After accepting the certificate from ESM Manager during the login process, that is, the first time this installation of the Console is connecting to the Manager, restart the Console for 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-40514 TTP#66766	On a 64-bit Macintosh, displaying online help in the embedded browser is not supported. Workaround: Use an external browser instead.
ESM-40506 TTP#66753	On the Macintosh platform, setting Safari as the preferred external browser using the Console's Preference menu (Edit>Preferences>Program) will result in the wrong URL. Workaround: Change the setting from the Console's Preference menu (Edit > Preferences > Program > Preferred Web Browser > External Browser) to open. Next, make sure Safari is the default browser in your Mac OS(Safari > Preference > General > Default) web browser.
ESM-40302 TTP#66337	The server.log showed an exception when a custom view dashboard was launched in FIPS mode. Custom view dashboards are not supported in FIPS mode.
ESM-39980 TTP#65708	The Console can become unresponsive if you are trying to 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. This is a display issue. You may ignore the duplicate rows.

Issue	Description
ESM-39829 TTP#65421	<p>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 of thousands of actors are deleted, the whole deletion period may last for hours because actor deletion launches a category model rebuild.</p> <p>There is no workaround so far in current implementation. Our current implementation sends deletion requests one resource a time.</p>
ESM-39331 TTP#64251	<p>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.</p>
ESM-39322 TTP#64233	<p>When viewing a Category Model, if the user is a non-admin user, a NullPointerException will be thrown by the Arcsight Console, even if the user has been given read and write rights on all the actors and the Actor Base field set.</p> <p>Workaround: View the Category Model as an admin user.</p>
ESM-39101 TTP#63834	<p>In Suite B mode, the custom view dashboard cannot be launched.</p> <p>Workaround: Use an external web browser. Go to Preferences &gt; Programs and deselect "Use the web browser embedded in ArcSight Console"</p>
ESM-38961 TTP#63568	<p>For image view mode, when a background file is uploaded, the Console does not provide an option for a location. The file automatically goes into the user's personal folder.</p> <p>Workaround: After the upload, the user can move the file to a preferred folder.</p>
ESM-38415 TTP#62565	<p>In an active channel, you cannot add global variables to the channel through the right-click option, Add Column. Only global variables already added to the current field set will be displayed.</p> <p>Workaround: Add the global variables you want for the channel to a field set, then choose that field set for your channel.</p>
ESM-38014 TTP#61931	<p>When a filter is moved from one group to another and data monitors that depend on that filter is packaged, exported, and re-imported on a different ESM installation, the data monitors may have missing filter attribute values.</p> <p>Workaround: Manually set the filter for these data monitors that are identified by the broken resource icon.</p>
ESM-37868 TTP#61659	<p>When a user modifies a case while a case channel is open and an inline filter is applied, no data appears. To successfully display available data, the case channel has to be refreshed.</p>
ESM-37344 TTP#60500	<p>On a Manager where a large number of cases reside in a single group, the user can't pick a case for "Add to Existing Case" rule action in the Rule editor. The reason is that the resource selector only shows leaf nodes when there are less than 1000 cases in a group. The scope of this bug actually goes beyond cases. It happens for all resources in ESM.</p> <p>Workaround: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.</p>
ESM-37079 TTP#59649	<p>Linux and Mac OS: Logger integration commands are not available from the context menu on the Channels tab of the ArcSight Console.</p> <p>Workaround: To run Logger integration command for these operating systems, use an external browser.</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>

Issue	Description
ESM-35998 TTP#56865	On Linux only: If you right-click on the port field in a channel and select Integration Commands > Portinfo (Linux), you will get an error.
ESM-35853 TTP#56430	The Aggregation tab is not working for the Report table template. Workaround: For the Aggregation tab to become active, a user must not only apply a function to a column but also select a grouping column.
ESM-35830 TTP#56367	ESM v5.0 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. Workaround: It is recommended 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.
ESM-35465 TTP#55476	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: The maximum number of open event channels (10) has been exceeded. Please close one or more individual event channels to continue." Workaround: Restart the Console.
ESM-34830 TTP#53912	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. 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.
ESM-33453 TTP#51094	On Unix systems: The drag-and-drop feature does not work on the Console. Workaround: Use the cut-and-paste feature instead.
ESM-33440 TTP#51072	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-33360 TTP#50968	If you delete an escalation-level notification resource, you will receive the error Group does not exist in the console.log file. This error is incorrect and can be ignored.
ESM-32705 TTP#49608	In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range. Workaround: Delete the existing color mapping and create a new one with the color mapping of your choice.
ESM-32489 TTP#49024	Using hotkeys with View Pattern and View Pattern with Filter is not supported in this release.
ESM-31127 TTP#45403	An embedded browser in the Console is not supported on the Linux 64-bit platform. Workaround: Use an external browser instead. You can set up the Console to use the external browser during installation.
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.

Issue	Description
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 ^VVsOXg4BABCAIEuBhILMyg= Enter "^VVsOXg4BABCAIEuBhILMyg=" in the query text field.

## ArcSight Database

Issue	Description
ESM-46556	<p>During the Oracle database installation, at the step when you are creating a database instance, the wizard does not warn you if you use an instance name with a space, for example:</p> <p style="padding-left: 40px;">arcsight db</p> <p>Oracle does not allow spaces, and therefore the instance creation will fail. Do not use spaces for database instance names.</p>
ESM-46503	<p>Due to an issue with Oracle 11g, documented in Oracle Metalink article 1173167.1, when installing Oracle 11g on Unix platforms, if the DISPLAY variable points to an invalid Xserver, the Oracle 11g installation will fail with an error like "...Xlib: connection to ":0.0" refused by server Xlib: No protocol specified" or "Exception in thread "main" java.lang.NoClassDefFoundError at java.lang.Class.forName0(Native Method)" in the &lt;ARCSIGHT_DB_HOME&gt;/logs/database.installation.log.</p> <p>Workaround: Unset the DISPLAY variable before starting the Oracle 11g installation.</p>
ESM-46330	<p>The command line function to archive, deactivate, or reactivate partitions does not work if non-default values of archive, retention, and reserve period days are used.</p> <p>Workaround: Use the Console to perform the task.</p>
ESM-39206 TTP#64037	<p>When querying events with conditions on Actor fields, SQL queries may run slow especially in the following cases:</p> <ul style="list-style-type: none"> <li>- List conditions are used.</li> <li>- Conditions on event fields are missing.</li> </ul> <p>In some cases, queries may even time out and not produce results.</p>
ESM-35884 TTP#56521	<p>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>Workaround:</p> <ul style="list-style-type: none"> <li>- While logged in as the oracle user, run the Partition Archiver as a standalone application with "arcsight agents" command;</li> <li>or</li> <li>- Switch to /bin/sh which is the default Oracle shell in /etc/passwd.</li> </ul>
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 install 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>

---

Issue	Description
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 "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-46717	<p>During ESM Manager or ArcSight Web installation on Windows 2008 R2, ESM Manager or ArcSight Web could not be set up as services, and neither one will start. The following workaround applies to both ESM Manager and ArcSight Web. Some of the steps will instruct you on what values to use for ESM Manager or ArcSight Web.</p> <p>Install ESM Manager or ArcSight Web as a Windows Service using the following are steps:</p> <ol style="list-style-type: none"> <li>Download and install the Microsoft Resource Tool Kit:  <a href="http://www.microsoft.com/downloads/en/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&amp;displaylang=en">http://www.microsoft.com/downloads/en/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&amp;displaylang=en</a>  This is a Windows 2003 installer but it also works for Windows 2008.</li> <li>From the command prompt (Start &gt; Run &gt; cmd), execute one of the following commands.  For ESM Manager:  <code>sc create ArcsightManager-5.0.1 binpath= "\$resource_install_loc\Tools\srwany.exe" start= auto</code>  For ArcSight Web:  <code>sc create ArcsightWeb-5.0.1 binpath= "\$resource_install_loc\Tools\srwany.exe" start= auto</code>  Note: The spaces after binpath= and start= are mandatory.</li> <li>Run the registry (Start &gt; Run &gt; regedit).  For ESM Manager, locate and select:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ArcsightManager-5.0.1  For ArcSight Web, locate and select:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ArcsightWeb-5.0.1</li> <li>Select Edit &gt; Key.  A new entry will be created under the key, allowing you to rename this entry. Rename as follows: <ol style="list-style-type: none"> <li>Rename it to Parameters.</li> <li>Double-click Parameters.</li> <li>On the right pane, right-click and select New &gt; String Value. Then rename to Application.</li> </ol> </li> <li>Edit the Application key as follows: <ol style="list-style-type: none"> <li>Right-click Application and select Modify.</li> <li>Enter the file-path in the Data Value as follows:  For ESM Manager, use  &lt;ARCSIGHT_HOME&gt;\bin\arcsight.bat manager  For ArcSight Web, use  &lt;ARCSIGHT_HOME&gt;\bin\arcsight.bat webserver</li> <li>Click OK.</li> </ol> </li> <li>Close regedit and start Windows Services (Start &gt; Control Panel &gt; Administrative Tools &gt; Services.</li> <li>Select and start the ArcsightManager-5.0.1 or ArcsightWeb-5.0.1 service.</li> </ol>



Issue	Description
ESM-46572	During an actor import using the Model Import Connector, some archive files may be saved with the file name extension, .bad. If those files are subsequently manually imported, in some cases the result may be incomplete actor information loaded into the database. This does not affect any actors that were successfully imported from the Model Import Connector. There is no known workaround at this time.
ESM-46045	Occasionally you will see inconsistent behavior with domain field population in the active channel and Event Inspector panel after restarting the ArcSight Manager. Domain fields do not get populated even though correct domain is picked.
ESM-41331 TTP#68451	After the resource validation process is run, assets that are actually invalid appear to be valid.  Workaround: Manually mark assets that are known to be invalid as invalid.
ESM-41272 TTP#68310	Asset Aging tasks will not proceed if you have disabled assets in the system. Workaround: Use one of two options: - Fix the invalid assets, or - Ignore the invalid assets by adding the following to server.properties: asset.aging.excluded.groups.uris=/All Assets/System Disabled/Disabled Assets
ESM-41215 TTP#68187	On SUSE 11, ESM Manager does not start automatically at system startup even if this option was selected during installation. Workaround: Start Manager manually.
ESM-41208 TTP#68173	If ESM Manager is started as a service on a Windows 2003 32-bit machine, the service cannot be started and an error message may be displayed, even though the ESM Manager is being started normally in the background. Confirm successful Manager startup by searching the Manager's <ARCSIGHT_HOME>/logs/default/server.std.log file for the word "Ready."
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	System zones were modified for this release. So, after importing packages or archives containing assets in zones that were modified those assets will become invalid.  Workaround: You need to manually fix the zone for these assets.
ESM-40815 TTP#67348	If a domain field in a filter or rule is deleted, and you re-create the field with the same name, it appears that you can successfully validate the filter or rule. However, the filter does not match or the rule will not fire.  Workaround: To prevent this, re-create the domain field, associate it with the same domain field set, then validate the resource.
ESM-37633 TTP#61154	After installing the Manager, you will see an error in the server.log file: [ERROR][default.com.arcsight.config.util.WebProperties][getPassword] com.arcsight.common.ArcSightException: Cannot handle the data which was obfuscated by old scheme  This message is harmless and can be safely ignored.

Issue	Description
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. Additionally, the Manager runs out of memory and therefore automatically restarts itself.</p> <p>Workaround: You may 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-36328 TTP#57661	<p>If the Manager receives a scan for a host that already exists in ESM and belong to a dynamic zone, but giving your new asset a unique domain name, this asset gets created. So, you end up having two assets with the same hostname and dynamic address but different domain names.</p>
ESM-35732 TTP#56123	<p>The Archive tool can sometimes fail to import entries into an active list if the active list cannot be accessed. In such situations, you will not see any errors, but the list does not get populated.</p> <p>Workaround: Import the same package a second time.</p>
ESM-35668 TTP#55969	<p>On Linux only: You may experience high CPU utilization on the ESM Manager. This may be specific to your system/hardware.</p> <p>Workaround: If you are experiencing performance issues, try updating your drivers or reinstalling the Linux operating system.</p>
ESM-33462 TTP#51112	<p>Stages resources are editable from the ESM Console, although these should not be moved or customized. (See ESM Console Navigator &gt; Stages resource tree.) Please keep stages provided as standard content in the given folders and do not move them into another folder. Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created. (For more information, See the "Standard Content" topic in the Console Help.</p>
ESM-31433 TTP#46276	<p>On Windows only: If you install the Manager as a service, you may see the following error when the Manager starts:</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 database 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 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 log:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Regenerate the index by issuing the following command from the Manager &lt;ARCSIGHT_HOME&gt;/bin directory:</p> <pre>arcsight searchindex -a create</pre>
ESM-30314 TTP#42730	<p>You cannot move an asset using Auto Zone if the asset is locked.</p>

Issue	Description
ESM-30008 TTP#41582	<p>Occasionally, when installing an exported package from a bundle file, you might receive the following error:</p> <p>Install Failed: Resource in broker is newer than modified resource.</p> <p>This error does not occur every time you attempt to install an exported package from a bundle.</p> <p>Workaround: Re-import the package.</p>
ESM-27414 TTP#35166	<p>If you are running the sendlogs wizard and you click Previous or Next, an error message says</p> <p>Error (Null)</p> <p>Workaround: Cancel the wizard and start again.</p>

## ArcSight Web

Issue	Description
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>
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 some will not display properly on the Web.</p> <p>Workaround: ESM Administrators can set row limits on Query Viewers to control chart displays on both the Console and ArcSight Web. Determine which Query Viewers you want to display as charts. From 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"> <li>1. Log in to the ESM Console, choose Query Viewers in the Navigator, and right-click the Query Viewer you want to edit.</li> <li>2. On the Query Viewer Editor, if Use Default is enabled, click to deselect it. Then enter a row limit of 100 or less.</li> <li>3. Click Apply or OK to save the changes.</li> </ol>
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><a href="http://www.adobe.com/go/6b3af6c9">http://www.adobe.com/go/6b3af6c9</a></p>

## Connectors

Issue	Description
ESM-41419 TTP#68697	<p>There is a limitation if a connector needs to send events to multiple ESM Manager destinations with different versions (v4.5 and v5.0, for example). The serialization framework uses the lowest common denominator version (v4.5 in this case) to serialize events prior to sending to them to the ESM Managers. This means only 4.5 events will be sent to both ESM Managers.</p>

## Installation and Upgrade

Issue	Description
ESM-46685	<p>During an upgrade from Oracle 10g to 11g, you get a TNS Listener error and cannot proceed with the upgrade.</p> <p>On Windows, prior to upgrading, remove the ORACLE_HOME environment variable, then reboot your server for the changes to take effect.</p> <p>If you have already upgraded and you are getting the TNS Listener error during post-upgrade tasks, do the following:</p> <ol style="list-style-type: none"> <li>1. Go to Control panel &gt; System &gt; Advanced &gt; Environment variable.</li> <li>2. Change the ORACLE_HOME variable to point to the new Oracle 11g home.</li> <li>3. Click OK to save.</li> <li>4. Click OK on the TNS Listener error pop-up. Then click Next.</li> </ol> <p>This should allow you to proceed with post-upgrade tasks and also complete your upgrade.</p>
ESM-46545	<p>After the 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 5.0 SP1 release to identify invalid assets.</p>
ESM-46402	<p>On systems set to French locale, there was a failure during ESM Manager upgrade from 4.5 SP3 Patch 1 to 5.0 GA Patch 1 and to 5.0 SP1. This error was seen at the upgrade step, "Transfer setting from source ArcSight Home."</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Back up the "archive" folder under manager ARCSIGHT_HOME/reports folder of the source Arcsight ESM Manager location.</li> <li>2. Delete the "archive" folder under manager ARCSIGHT_HOME/reports folder of source Arcsight ESM Manager location. (Required only if you run into an issue.)</li> <li>3. Resume ESM Manager upgrade by running this command in &lt;ARCSIGHT_HOME&gt;/bin:  <pre>arcsight upgrade manager</pre> </li> <li>4. After a successful ESM Manager upgrade to 5.0 patch1 to 5.0 SP1, copy the "archive" folder from the backup location and paste it under the ESM Manager upgrade location:  <pre>&lt;ARCSIGHT_HOME&gt;/reports of 5.0 Patch1/5.0 SP1</pre> </li> <li>5. Start ESM Manger.</li> </ol>
ESM-46376	<p>During an ESM Database upgrade from Oracle 10g to Oracle 11g, the wrong Oracle home value is shown as the default location. This issue appears during an ESM Database upgrade from Oracle 10g to Oracle 11g, after you have performed the Transfer Partition Archiver Settings task. At the point during Oracle 11g installation, make sure you enter the correct destination for Oracle 11g home. By default, the destination shows as c:\oracle\OraHome10g. If you keep this default, your Oracle 10g files will be lost. You must therefore change the destination to OraHome11g, for example, c:\oracle\OraHome11g.</p>
ESM-46263	<p>If you try to install oracle 10g and 11g on different drives and upgrade from 10g to 11g, there will be issues with TNS listener startup. Try to install 11g on same drive as 10g.</p>
ESM-41220 TTP#68193	<p>When upgrading packages, the upgrade summary report that provides a list of installed packages may show packages that were not installed after all. You should ignore this. The summary report is in error in this case. Most likely, you did not have those packages prior to the upgrade.</p>

Issue	Description
ESM-41148 TTP#68075	<p>During an upgrade to ESM 5.0 GA, autozoning will fail if the number of assets in a zone/group exceeds 1000.</p> <p>Workaround: If this happens, 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. Generally, you would 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 ESM v4.0 SP3, v4.5 SP1, or v4.5 SP2 to ESM v5.0 GA 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. In &lt;ARCSIGHT_HOME&gt;/&lt;Console_Build&gt;/current/bin, run the arcsight consolesetup at the command line. This way, SSL files are read and the Console can 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 &lt;ARCSIGHT_HOME&gt;/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 or ArcSight Web server. If there are spaces in the install paths, ESM Database, Manager, 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>
ESM-34069 TTP#52690	<p>This release does not support spaces in install paths for the ArcSight Database, ESM Manager or ArcSight Web server. If there are spaces in the install paths, ESM Database, Manager, 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: Please do not use spaces in ESM installation paths. The default install paths (for example, 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>
ESM-34011 TTP#52556	<p>You will not be able to do two consecutive upgrades on the same day. For example, upgrading from v4.5 SP1 to v4.5 SP2, then upgrading to v5.0 cannot be done on the same day.</p> <p>Workaround: After doing one upgrade, wait until the execution of the next scheduled Partition Manager job before doing the next upgrade. This allows Partition Manager to create a new partition which allows the system to be recognized as upgraded to an intermediate version. Execution of the Partition Manager scheduled job can be ensured by letting the Manager from the first upgrade run for a day (24 hours). Do the next upgrade after a day.</p>

Issue	Description
ESM-33949 TTP#52394	<p>File resources are not handled properly during ESM upgrading. This results in unassigned file resources after the upgrade. For example, .art files are created as new file resources in ESM v4.5 SP1 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-33766 TTP#51954	<p>This release does not support spaces in install paths for the ArcSight Database, ESM Manager or ArcSight Web server. If there are spaces in the install paths, ESM Database, Manager, 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 (for example, C:/arcsight/Manager) do not include spaces. If you modify the install paths, make sure there are no spaces in the directory names. Use dashes (-) or underscores (_) instead of spaces.</p>
ESM-31766 TTP#47206	<p>During an upgrade to v4.5 SP1, the "SSL Client Only" authentication option is selected by default. If you had set up your v4.0 SP3 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-31728 TTP#47129	<p>Windows only: When installing or upgrading, the Partition Archiver Wizard gives you information in the last screen of the wizard to install it as a service, even if you chose to not install it as a service. Ignore this information and continue with the installation/upgrade.</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. 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-46567	In a localized environment, the Group variable functions, for example GetGroupsOfAsset and FormatGroupsOfAsset, do not return results in active channels.

## Pattern Discovery

Issue	Description
ESM-46312	If you create a rule from patterns that use domains, you must aggregate the field, Domain Name. If this field is not aggregated, the rule will not be fired.
ESM-46250	In ESM 5.0 SP1, if a domain field is shared by more than one domain, the event graph is not shown correctly.
ESM-46157	In Profile "Actions" tab, Global Variables are unavailable for "Add to Active List" and "Add to Session List" actions. For example, when "Add to Active List" is selected for "On Pattern Discovered" action, the Active List and the Active List field mappings need to be provided. In the drop-down menu of the field mapping, the Global Variables are disabled.
ESM-35048 TTP#54452	A java.lang.InterruptedException might be logged in the ESM Manager server.std.out.logs 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.
ESM-20555 TTP#24715	In pattern discovery, if a profile has event fields with the same name as an event annotation stage name, the snapshot will show a null in the resulting event fields. The snapshot will not be forwarded to the event graph.



## Issues Fixed in ESM 5.0 SP1

The following issues were fixed in this release. The links are sequenced according to the workflow of installing, configuring, and using ArcSight ESM features:

- ["Installation and Upgrade" on page 36](#)
- ["ArcSight Manager" on page 34](#)
- ["ArcSight Database" on page 34](#)
- ["ArcSight Console" on page 32](#)
- ["Analytics" on page 30](#)
- ["ArcSight Web" on page 36](#)

## Analytics

Issue	Description
ESM-45698	Ignoring invalid resources caused aggregated events to not populate customer defined user zones. This is now fixed.
ESM-41706 TTP#69792	You now have the ability to compare numeric field values of different numeric types, for example, long compared to floating point type.
ESM-41139 TTP#68054	While you can create a trend on data of type resource ID (e.g., Domain ID) and gather data on those fields, you will be unable to see them in the trend grid or construct a query on them. If you want to have the resource ID information, you should use the resource reference field (e.g.: Domain). Other fields like resource ID, URI, NAME, and so forth, can be derived from this field.
ESM-40980 TTP#67792	There is inconsistency in how variables are evaluated across resource channels: <ul style="list-style-type: none"> <li>- In actor channels, variables are evaluated accordingly.</li> <li>- In case channels, a message states that variables are not supported and won't be evaluated. However, the channel displays a Variable column which is empty.</li> <li>- In asset channels, a message states that variables are not supported and won't be evaluated. However, the channel displays a Variable column which has values.</li> </ul> This is expected behavior.
ESM-40807 TTP#67328	Aggregate on the Domain Resource field to populate domain fields in correlation events: Domain fields are set only in the context of a domain. Therefore, user must aggregate on the domain resource field while aggregating on domain fields to have the domain fields populated in the correlation event.
ESM-40599 TTP#66925	To add global variables to an active channel, the variables need to be part of a field set.
ESM-40213 TTP#66129	Previously, the category model function HasRelationship used to build local or global variables returns a Boolean value (0 or 1). This is not supported in query viewers and including such a variable in the query for the query viewer will result in an error. <p>If your query uses a global or local variable with function HasRelationship, the report shows 0 for false and 1 for true. If you create a query viewer on the query, the query viewer will not load. For this release, the function HasRelationship is useful for the evaluation of conditions rather than as a selection column for queries.</p> <p>In this release, this is no longer a problem.</p>
ESM-40212 TTP#66128	Previously, you could not create a query viewer using a category model global variable. Now, you have the ability to do this.
ESM-38915 TTP#63477	Scheduled rules using domain fields in their condition are not fired.
ESM-38421 TTP#62574	Populating an event based active list with "resource ID" type fields was formerly unsupported, for example the "Domain ID" field. This is now supported.

Issue	Description
ESM-37960 TTP#61827	If you build a query on actors and you select a user-created data list variable such as GetActiveListValue or GetSessionData, the variable will not be displayed with the dot notation as seen in other resources. Data list variables (whether local or global) have fields; for example, if you have an active list called Watched Accounts with two columns, username and host, and you define a GetActiveListValue variable called GetWatchedAccount, you will have two fields to choose: GetWatchedAccount.username and GetWatchedAccount.host. This is what normally happens for other resources. For actors, you will only see username and host without the prefix.

## ArcSight Console

Issue	Description
ESM-45937	After applying v5.0 patch 1, when you connected to the ESM Console and launched either a custom view dashboard or an external browser, the system displayed a blank screen. This happened only on first connection after an upgrade or a fresh installation where you imported the Manager certificate using the Console wizard screen that prompts you to select your authentication type.
ESM-45909	If values were entered in Longitude and Latitude fields of the Common Conditions Editor, the user has to click on some other field before the values can be applied. The issue is fixed.
ESM-45767	An error occurred whenever an imported package added a rule to a real-time rule group that previously existed but was empty (contained no rules). The rule(s) added to the group become invalid as a result. The workaround was to manually validate the rule(s) after the import.
ESM-45738	<p>The internal browser does not start on 32-bit Linux 5.X when using a previous version of Firefox. To fix this, edit the Firefox file,</p> <p><code>/usr/lib/[FIREFOX_FOLDER]/application.ini</code>. Change <code>MinVersion=1.9.0.12</code> to <code>MinVersion=1.9.0.11</code>.</p> <p>Alternately, you can install the latest version of Firefox and change your Console settings to point to that version.</p>
ESM-41207 TTP#68170	When used in a filter, the <code>inActiveList</code> condition with a list parameter ignores the setting, "All values must match." If that box is checked, the condition will apply if any (instead of all) of the items in the list match. This condition can no longer be reproduced.
ESM-41018 TTP#67855	The image dashboard feature does not work if your ESM installation is configured with Password and SSL Authentication. If you launch an image dashboard, you will receive an error stating that there is an error opening the custom layout because of an invalid authentication token.
ESM-41011 TTP#67842	<p>Charts are not visible but the tables are, when using the custom view dashboards in the embedded browser. The embedded browser does not have required Adobe Flash plugin.</p> <p>Workaround: Install Mozilla Firefox 2 or 3 and download Adobe Flash Player. Restart the Console if necessary. JxBrowser in the embedded browser then copies the Adobe Flash Player. No other changes to preference settings are required. If this workaround solves the problem, you may continue to use IE. You may also uninstall Firefox.</p>
ESM-40978 TTP#67790	<p>There is inconsistency in how variables are evaluated across resource channels:</p> <ul style="list-style-type: none"> <li>- In actor channels, variables are evaluated accordingly.</li> <li>- In case channels, a message states that variables are not supported and won't be evaluated. However, the channel displays a Variable column which is empty.</li> <li>- In asset channels, a message states that variables are not supported and won't be evaluated. However, the channel displays a Variable column which has values.</li> </ul>
ESM-40696 TTP#67115	If you create a query on a field-based active list whose field names begin with domain (for example, <code>domain1</code> , <code>domainfieldstring1</code> , <code>domainstr1</code> ), clicking Add Select columns in the Field tab from Query Editor will not display the field names that begin with domain. This means your queries will not be able to search on these field names.
ESM-40369 TTP#66475	When running the Network Maps TRM command using the internal browser, an error message about one or more ActiveX controls is displayed. Now, you can check the option "Allow ActiveX to run in the embedded in AcrSight Console" from the Edit > Preference > Program menu.

Issue	Description
ESM-40187 TTP#66086	In a category model, using buttons to expand or collapse one level works the first time. Using the buttons again will cause the category model view to zoom out. The buttons are designed for collapsing or expanding the graph and may not work as expected as you drill down.
ESM-39321 TTP#64232	In the Actors resource, non-admin users can now view actors in the actors channel if given read and write permissions to the Actors resource and the actor base field set.
ESM-39218 TTP#64052	In some contexts, entering literal string values containing commas results in the string being interpreted as a list, notably when they are arguments to list operators such as "intersectsList." This may arise in particular when trying to enter Distinguished Names (DNs) in the context of Actors, for instance:  accountID intersectsList CN=USER3119,OU=OU_ESMQA_10K,DC=MOM2007,DC=SV,DC=ARCSIGHT,DC=COM  The values entered by the user are now preserved.
ESM-37896 TTP#61699	When the @ symbol all by itself is used in the Query's condition tab, enclose the symbol in double quotes for the condition to work:  "@"  For example, your condition is Name Contains "@"  This applies only to the Query resource.
ESM-37752 TTP#61438	From the Logger search page embedded in the ESM Console, there is the ability to launch an external browser. The password is then exposed on the URL. This has been fixed on the ESM side.
ESM-37050 TTP#59513	Device Custom date fields can now be selected in the Aggregation tab and for the Set Event Field action in the Rule Editor. This allows setting of Device Custom Date fields in the correlation event using the values in base events, for use in rule actions, for example, adding the value to an Active List. The functionality was made available in ESM 5.0 release.
ESM-36908 TTP#58997	Device Custom date fields can now be selected in the aggregation tab as well as Set Event Field Action in Rule Editor. This allows setting of Device Custom Date fields in the correlation event using the values in base events, for use in rule actions, such as adding the value to an active list. The functionality was made available in ESM 5.0 release.
ESM-28093 TTP#36436	The new "New Search Group" feature allows you to create groups in the Cases resource that automatically query cases based on the conditions provided in CCE of that Case search group.

## ArcSight Database

Issue	Description
ESM-34066 TTP#52680	This release does not support spaces in install paths for the ArcSight Database, ESM Manager or ArcSight Web server. If the administrator enters spaces in the paths during installation, the installation wizard displays an error.

## ArcSight Manager

Issue	Description
ESM-46201	Base events are not exported when exporting to an external system from channel or rule. If your external ticketing system integration use case requires access to base events, contact ArcSight Support to obtain a fix for this issue.
ESM-46075	After restarting the Manager, the Rule that contains domain field in the condition did not trigger.
ESM-41407 TTP#68655	<p>If you have a large amount of resources and additionally have 50 K or more actors in the system, and you are running a search, you may run into this error that includes:</p> <p>... Search index utility completed: com.arcsight.tools.process.ProcessTimeoutException: Command did not finish in time.</p> <p>Your searches may not return the expected results.</p> <p>Workaround: Regenerate the index by issuing the following command from the Manager's &lt;ARCSIGHT_HOME&gt;/bin directory:</p> <pre>arcsight searchindex -a create</pre>
ESM-41221 TTP#68194	For large numbers (in the thousands or more) returned by data monitor, an enhancement was introduced. For better readability, the large numbers now use comma separators.
ESM-41043 TTP#67895	<p>After importing the ArcSight JumpStart for Perimeter Monitoring 1.0 package and configuring the Perimeter Monitoring use case, the data monitor and dashboard resources become invalid.</p> <p>The issue was caused by a fault in the archive import process that under certain circumstances triggered the loss of resource IDs. That, in turn, caused the resource reference check to fail; as a result, the corresponding resources were marked as invalid.</p> <p>The package importing process has been corrected to keep track of the Resource ID all the time during the import operation.</p>
ESM-40975 TTP#67777	<p>After uninstalling then re-installing the ArcSight Administration package, you will get invalid resources.</p> <p>An unguarded access to the Table Schema resources caused a race condition and triggered the database integrity protection mechanism; as a result, some resources from the ArcSight Administration package were marked as invalid.</p> <p>The access to the Table Schema resources has been safeguarded against attempts to modify data simultaneously.</p>
ESM-38274 TTP#62342	In FIPS mode, the required runtime libraries to run VC++ 2005 are now part of the installation.

Issue	Description
ESM-35918 TTP#56639	<p>If using Mozilla Firefox 3.08 to connect to ArcSight Web, you will get an error. This is a known limitation if ESM Manager and ArcSight Web are configured to use FIPS.</p> <p>Using Internet Explorer 6 configured to use SSL 3.0 and TLS 1.0 encryption does not produce the error. See the chapter "Installing ArcSight Web" in the ESM Installation and Configuration Guide for details on configuring Internet Explorer.</p>
ESM-33039 TTP#50301	<p>A trend failed with an error saying that the value was too large for the column. This error was fixed by adjusting the column sizes for URL Filename and URL Query. This fix affects new trends only. Trend tables prior to ESM v5.0 SP1 will not be changed. Additionally, if a package is imported, the column size defined in the package will not be upgraded to the changed column sizes.</p>

## ArcSight Web

Issue	Description
ESM-39307 TTP#64207	When adding correlated events to a case using ArcSight Web, your only option on the Edit panel was either to add to an existing case or create a new case. You did not have the option to include a base event. Now, a checkbox is added to ArcSight Web that allows you to add a correlated event's base events to a case.
ESM-31690 TTP#46969	When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an Active Channel. This error can no longer be reproduced.
ESM-20888 TTP#25121	After upgrading to ESM 4.5 and if the user used different logo, that custom logo did not carry over. After the browser was started, ArcSight Web showed the default ArcSight logo. This is now fixed. The custom logo will be used.

## Installation and Upgrade

Issue	Description
ESM-46655	<p>During an upgrade from ESM v5.0 GA to ESM v5.0 SP1, the upgrade failed for the zone resource with the cardinality conflict. This is because the same zone showed up in a network twice.</p> <p>In this case, you need to go back to a pre-upgrade version and find out the parent groups of the zone belongs to the same network. If so, remove the zone from groups and make sure the zone's parent group shows up in network only once.</p>
ESM-46644	The Installer is showing "Available: Error!" for disk space information during installation of ArcSight Database, Manager and Web. This is the behavior in console mode installation. In GUI mode, the error is not displayed. This problem is due to Install Anywhere and cannot be fixed.
ESM-46406	<p>This problem was found in Linux systems set to the French locale and only if users were upgrading from v4.5 SP3 patch1 to v5.0 Patch1. The ESM Manager, Console, and Web did not automatically pick up the French locale after startup. English was still used.</p> <p>As a workaround, after the upgrade from v4.5 SP3 Patch1 to v5.0 Patch 1 and before starting ESM Manager, Console, and Web, the users were required to add the following two lines in the <code>.bash_profile</code> file found in the <code>&lt;USER_HOME&gt;</code> folder:</p> <pre>LANG=fr_FR.UTF-8 export LANG</pre> <p>After the changes, users needed to start Manager and make sure all configurations are working correctly. Then, before upgrading ESM Manager, Console, and Web from v5.0 Patch 1 to v5.0 SP1, users then needed to remove the lines added in the workaround. That means they had to remove the lines,</p> <pre>LANG=fr_FR.UTF-8 export LANG</pre> <p>from the <code>.bash_profile</code> file.</p>
ESM-45943	After applying the patch on the Manager, the <code>server.xml</code> file gets overwritten. So, on AIX, if you had changed the port for the service layer in <code>server.xml</code> , you will need to make that change in <code>server.xml</code> file after applying the patch.



Issue	Description
ESM-45617	<p>You might see such messages related to licenses at some places in our log files. You can ignore these messages as they are harmless.</p> <p>INFO: License client supports keys: [ENTERPRISE, QA]</p>
ESM-41297 TTP#68352	<p>While upgrading to ESM v5.0 GA, the logs may show a database exception about CAT_DEVICE_TYPE invalid identifier. This field is not required by the upgrade. The upgrade will complete successfully and ESM Manager will initialize with no problems. You should ignore this exception.</p> <p>This issue does not apply to an upgrade from ESM 5.0 to ESM 5.0 SP1.</p>
ESM-41201 TTP#68161	<p>ESM Database installations on SUSE platforms:</p> <ul style="list-style-type: none"><li>- SUSE 11 is a supported platform for ESM 5.0 Database installations. However, you will see a prompt at installation saying that it is not supported. Proceed with the installation by clicking OK.</li><li>- SUSE 10sp2 support in ESM 5.0 Database installations will End-of-Life on March 1, 2011. The installer program will not warn you of this fact if you install after that date.</li></ul>

