Release Notes
ArcSight™ ESM

Version 5.0 GA

June 14, 2010

Release Notes ArcSight™ ESM ,
Version 5.0 GA

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
09/24/10	ArcSight™ ESM Version 5.0 GA	Put in the fix for the Jira bug, ESM-41526
06/14/10	ArcSight™ ESM Version 5.0 GA	Release Notes for ArcSight™ ESM Version 5.0 GA.

ArcSight Customer Support

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

Contents

ArcSight ESM, Version 5.0 GA

Welcome to ArcSight ESM, Version 5.0 GA

ArcSight Enterprise Security Management (ESM) v5.0 introduces a new feature set that broadens its security and event management platform and its identity correlation functionality. This functionality includes user modeling through Actors, a customizable event schema and improved variable authoring through the introduction of global variables. ArcSight ESM v5.0 also includes enhancements in the area of custom view dashboards, field-set authoring, active list enhancement, Suite B encryption support, and event case preservation and reporting.

What's New in This Release

This release introduces a new feature set as outlined below:

Actors

ESM v5.0 introduces a new feature called Actors that provides a new way of mapping users and their behaviors to their application and network activity enabling easy to configure correlation analysis. With the assistance of the Actor Model Import Connector customers are able to populate and maintain the Actor model in sync with their Identity Management System such as Active Directory.

Actors is a separately-licensed feature made available with an IdentityView Solution purchase.

Domain Field Sets

ESM v5.0 introduces the concept of domain field sets which allows you to uniquely identify and group events with common attributes relevant to a business vertical, such as transaction monitoring (for example: credit card, online banking, or stock transactions). Domain field sets make it easy to monitor, correlate, and analyze events not only for traditional security use cases, but also for any specialized business-related use cases.

Domain field sets is a separately-licensed feature made available with a FraudView purchase.

Global Variables

Global variables introduces the ability to author variables which derive particular values from existing data from a centralized location and re-use them in multiple places, simplifying the content authoring process. As part of global variables, ESM v5.0 also introduces the ability to promote resource specific variables into global ones by a simple click of a button.

ESM Service Layer

As part of this release, ESM introduces a new service layer which enables customers to integrate their own applications with the product through functionalities such as Web Services. ESM Service Layer uses a service-oriented architecture (SOA) that supports multiple Web Service clients written in different languages.

Suite B Support

As part of ESM v5.0, ArcSight introduces the ability to deploy the product and all of its corresponding components to the Suite B supported cryptographic algorithms. Suite B is a set of cryptographic algorithms put forth by the National Security Agency (NSA) as part of the national cryptographic technology.

ArcSight ESM v5.0 System Enhancements

This release introduces enhancements as outlined below:

Manager Enhancements

- **Schema and data type expansion**

  As part of ESM v5.0, the security event schema has been enhanced to be more flexible, extensible, and customizable for ranges of application beyond traditional network security. ESM v5.0 base schema now offers:

  - IPv6 and Floating points field type support
  - Custom string fields has been increased to 4000 bytes support
  - Additional schema, custom and category fields

- **Asset aging**

  ESM Asset management has been enhanced to offer the ability to update the asset model confidence factor based on an assets age based on its last scan update and delete/expire an asset past a certain age.

- **Case event preservation**

  ESM v5.0 introduces the ability to preserve the event associated with a case beyond the event retention policy.

- **Reusable field sets**

  As part of ESM v5.0, field sets have been broken out into their own resource enabling the creation of custom field sets based on the resource type (for example, actor, cases, and event field).

Correlation Enhancements

- **Active lists**

  Active lists offer support for multi-mapping of a key field to multiple values which return as a list through the introduction multi-map active lists. Active lists have also been enhanced to offer partially cached active lists which will store and retrieve additional entries beyond the in-memory from the database.

- **New variable functions**

  ArcSight ESM v5.0 enhances variables with the following functions:

  - Timestamp functions

    - Get Year
    - Get Day of Year
  - Alias

    Alias Field
  - Type conversions
    - String to List
    - Convert Address to String
  - String functions

    Concatenate Three
  - Actors

    Has Relationship
- Trend actions

  As part of ESM v5.0, trends have been enhanced to offer the ability to populate active lists with trend data, making trend results readily available for use in rules, filters, active channels, etc.

Console Enhancements

- **Custom view dashboards**

  Dashboards have been enhanced to offer support for custom views, which enable users to create custom layout views for dashboards and display data monitors over an imported image.
- **Data monitor drill-downs**

  Data monitors have been enhanced to offer the ability to select a field set for drilling down, which enables users to define specific columns (fields) to be shown in the drill-down channel.
- **Query editor**

  The ArcSight ESM v5.0 query editor has been enhanced within the query definition panel. The Select, Group By, and Order By fields have been improved for ease-of-use with drag-and-drop capability and all three options are on a single view.

Upgrade Support

The following upgrade paths are supported for this release:

- ESM v4.0 SP3 to v5.0 GA
- ESM v4.5 SP1 to v5.0 GA
- ESM v4.5 SP2 to v5.0 GA

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

New Platform Coverage

Please review the ArcSight ESM v5.0 GA 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:

- **SUSE Linux 11 Enterprise Server 64-bit**

ArcSight ESM v5.0 GA Manager, Database, and ArcSight Web support is offered for SUSE Linux 11 Enterprise Server 64-bit.

- **Microsoft Windows Server 2008 SP2 64-bit**

  ArcSight ESM v5.0 GA ArcSight Database support is offered for Microsoft Windows Server 2008.

- **JRE Support**

  ESM v5.0 GA provides support for JRE 1.6., update 17.

Section 508 Compliance

ArcSight recognizes the importance and relevance of accessibility as a product initiative. To that end, ArcSight is making and continues to make advances in the area of accessibility in its product lines.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20100401.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort Sourcefire SEU 316	Faultline, Bugtraq, CVE, Nessus, MSSB
Enterasys Dragon IDS	Faultline, Bugtraq, CVE, MSSB, CERT
Cisco Secure IDS S483	Faultline, Bugtraq, CVE, Nessus
TippingPoint UnityOne DV7988	Faultline, Bugtraq, CVE, MSSB
Fortinet Fortigate	Bugtraq, MSSB
IBM/ISS SiteProtector	Faultline, Bugtraq, CVE, X-Force, CERT, MSSB
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, Nessus
Radware DefensePro	Faultline, CVE, Nessus
FunkWerk (VarySys Technologies) PacketAlarm	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB, MSKB

Oracle Critical Patch Update (CPU) Certification

This release of ArcSight ESM has been certified with the Oracle critical patch update (CPU) for April, 2010. Certification has been established with Oracle 10.2.0.4. Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

Platform	CPU April 2010 Patch
Windows 32	p9393548_10204_Win32.zip

Platform	CPU April 2010 Patch
Windows 64 (AMD64-EM64T)	p9393550_10204_MSWIN-x86-64.zip
Linux 32	p9352191_10204_Linux-x86.zip
Linux x86-64	p9352191_10204_Linux-x86-64.zip
AIX	p9352191_10204_AIX5L.zip
Solaris 64	p9352191_10204_Solaris-64.zip

OPatch

Visit the ArcSight Customer Support product-download site to get the correct Oracle CPU package and OPatch for your environment.

Platform	OPatch April 2010
Linux 32	p6880880_102000_LINUX.zip
Linux x86-64	p6880880_102000_Linux-x86-64.zip
Solaris 64	p6880880_102000_SOLARIS64.zip
Windows 64 (AMD64-EM64T)	p6880880_102000_MSWIN-x86-64.zip
Windows 32	p6880880_102000_WINNT.zip
AIX	p6880880_102000_AIX64-5L.zip

To Apply the CPU

1. From the Product Download section of the ArcSight Customer Support site (https://support.arcsight.com/), download both the Oracle CPU and OPatch:
   - Download the correct Oracle CPU package for your platform (see the tables above) and unzip the files under your working directory.
   - Download the Oracle 10g OPatch file for your platform.
2. Install the OPatch:
   - Review the `README` file in the OPatch zip archive.
   - Extract the contents of the OPatch zip file under `$ORACLE_HOME`.
3. Stop the ArcSight Manager and Partition Archiver, and also stop the Oracle instance and TNS Listener.
4. Set the OPatch binary in PATH.
5. Read the next section in this document, "Workarounds for Known Issues in Oracle CPU" on page 6.
6. Install the CPU (that you downloaded in Step 1) according to the steps outlined in the `README` in the CPU zip package for your platform.
7. Replace references to "OPatch" in the commands with
   `$ARCSIGHT_HOME/bin/arcdbutil patch`

   where `$ARCSIGHT_HOME` refers to the location where the ArcSight Database is installed.

For example,

On Windows:

If the `README` says:

```
>OPatch apply
```

use this command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch apply
```

On UNIX:

If the `README` says:

```
>opatch napply -skip_subset -skip_duplicate
```

use this command instead:

```
$ARCSIGHT_HOME/bin/arcdbutil patch napply -skip_subset
-skip_duplicate
```

> **Note** More information about Oracle-specific steps is provided in the README that accompanies the Oracle CPU. Be sure to review the README carefully and follow those instructions.

8. To complete the installation, follow the “Post Installation Instructions...” steps in the `README`.
9. Restart the database and the TNS Listener.
10. Restart the Partition Archiver and the ArcSight Manager.

Workarounds for Known Issues in Oracle CPU

The following subsections provide workarounds for issues related to the Oracle CPU on different platforms.

Windows for Oracle 10g

In some cases, the CPU application might fail and the following error message appears.

```
OUI-67124:Copy failed from "<source>" to "<destination>"

OPatch failed with error code 115
```

This error occurs when there are other processes running that lock the file in question. The processes that cause the lock might be related to Oracle. As a workaround, reboot the machine and try the patch application steps again.

Linux - Using a Large Instance

If your ArcSight Database is running on a 32-bit Linux machine with the SMP kernel and your system is configured to use between 2 GB and 4 GB of memory (the default configuration of the Large template), perform the following steps after applying an Oracle Patch or an Oracle Patch Set (for example, a Critical Patch Update or the patch set for 10.2.0.4) to your ArcSight Database.

1. Log into the database machine as the Oracle software owner (by default, Oracle).

2 Shut down the Oracle database, the TNS Listener, and all other Oracle services (if any).

3 Run these commands:

```
cd $ORACLE_HOME/rdbms/lib

mv ksms.s ksms.s.org; mv ksms.o ksms.o.org

$ORACLE_HOME/bin/genksms -s 0x15000000 > ksms.s

make -f ins_rdbms.mk ksms.o

make -f ins_rdbms.mk ioracle
```

4 Restart the database server and the TNS Listener.

Restarting the database server enables the ArcSight Database to utilize the extended memory. Oracle cannot restart if this procedure is not followed. If the above commands display errors, call ArcSight Customer Support. If you are using your own Oracle software license, contact Oracle.

Usage Notes

ESM v5.0 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.

Actors and Category Models

It is possible that during the actor import process from the Actor Model Import connector, one or more actor import files containing data for multiple actors may not have imported successfully into the Manager. This can happen because of network connection problems, an out-of-memory error, or some other problem that caused the import of that file to fail. Please see bug number "66978" on page 18 for more details on this.

Category models are in beta state. ArcSight recommends defining two to three category models at the most.

Domain Field Sets

Domain Field information is contained in the AdditionalData structure. However, you may have additional data that are not Domain Fields which you would like to persist in the AdditionalData table. In this case, ArcSight recommends that the length of the name of the AdditionalData be 40 characters or less. Anything more than 40 characters will result in the event not being persisted.

Domain fields are not supported in event-based active lists and Pattern Discovery. An event-based active list cannot be populated if it contains a Domain field. Pattern Discovery does not support domain field sets.

Global Variables

Variables using Group, List, and Category Model functions are evaluated on the Manager, not directly on the Console, and are referred to as "remote" variables.

These remote variables are evaluated only once on the console for any given event or resource. Therefore, the value of the variable on the Console will not change if the underlying data is modified that would result in a different value for the variable. New events (in events channels) and resources (in resource channels) will evaluate the variable again, and you will see the updated value.

Because not all variables can be calculated on the Console, there may be a delay in returning values from variables calculated "remotely" on the Manager.

Asset Aging

After the upgrade and before running any asset aging tasks, manually validate your assets by running the following command from the Manager's `/bin` directory:

```
arcsight resvalidate -persist
```

This is important especially if you have assets in the system zones.

Embedded and External Browsers

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

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

On 64-bit platforms, use the 32-bit version of the browser.

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

ArcSight Web

ArcSight Web provides monitoring and investigation access to data derived from global variables in dashboards, channels, and reports.

Data fields derived from global variables provide the same drill-down investigation from active channels and dashboards that regular event fields do.

Global variables operate on regular event fields, assets, cases, and actors. For more about monitoring and investigating events from ArcSight Web, see the ArcSight Web User's Guide.

Query Viewers

Query viewers and channels display results from variable calculations differently. For example, a value may be displayed as `-0.1` in a query viewer, and `-0.099999999999`... in a channel. Please see bug number "62109" on page 16 for more details on this.

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.

Documentation-Related Notes

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

- The standard content that supports tracking actor configuration changes has been updated from the lists published in the ESM User Guide (Actors > Actor-Related Resources Provided in Standard Content > Tracking Actor Configuration Changes Using Standard Content).
- The following steps for how to create an asset filter were inadvertently left out from the documentation.
  - **a** In the Navigator panel, go to Assets. Right-click any group and select **New Group**
  - **b** Add one or more assets to the new group

c. Highlight the new group, right-click and select **Show Filter**. The results will display in the Viewer panel.

d. In the Viewer panel, right-click the filter and select **Save Filter**. Give the filter a name.

e. In the Navigator panel, go to filters. You can edit the new filter by double-clicking it, or right-click and select **Edit**.

f. Remove the condition for the asset group ID that has only resource ID.

g. Select Asset tab, add the same asset Group with a name of the resource group from the drop-down menu.

h. Click **Apply** to save the selected asset group

i. Click **Apply** to save the filter

- Steps to troubleshoot why a domain field isn't populating when you think it should.

  a. Temporarily enable additional data persistence in server.properties to allow troubleshooting (requires Manager restart):

  `turbo.enabled=false`

  b. Ensure that the additional data name and domain field name match exactly. Field names are case-sensitive.

  c. Check that the data type set for the data on the FlexConnector matches the data type specified for it in the domain field. ESM writes a log entry every 15 minutes that indicates whether a domain field name matches, but the data type doesn't.

  Search the ArcSight log file for the following text:

  "`AdditionalDatas had processing errors`"

  d. Verify that the event is relevant to the domain.

  By default, ESM considers an event relevant to a domain if 80% of the event's additional data belong to that domain. For example, if an event has 10 additional data fields, at least 8 of them must match the domain fields in the domain field set.

  The default property can be changed in server.properties:

  `domain.event.relevance.percentage=0.8`

  e. Reset `turbo.enabled=true`; restart the Manager.

- The *ESM User Guide* topic Creating Rule Actions > Rule Actions > "Create a New Case" and "Add to Existing Cases" contains an example for calculating a case name dynamically. That example uses the static case name "Suspicious Login Attempts," and instead, the example should show a dynamic name, such as "Suspicious Login Attempts ${GetMonth}" where GetMonth is a variable name.

  On selecting the option "Calculate case name dynamically", the rule action will evaluate the dynamic case name and will pick the existing case with the matching with the name.

- Make note of the following updates about the custom view dashboards interface, which may differ from what is published in the ESM v5.0 User Guide:

  - To activate a context menu, use Alt + left click.
  - Custom view dashboards do not support drill-down on events.

- User has to refresh the dashboard manually to see a change made from another Console.

Open Issues in v5.0 GA

The following issues are either new or carried forward from previous ESM releases and remain open in v5.0 GA. These open technical issues merit your review to avoid difficulties.

Installation and Upgrade

Number	Description
39829	**On Linux only:** While running `runconsolesetup.sh` in the console mode, you will see an error message: `chmod: cannot access '/arcsight/Console5199/current/config/console.properties: No such file or directory` Ignore this message and continue with the setup. The setup will not be affected.
46153	**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.

46276	**On Windows only:** If you install the Manager as a service, you may see the following error when the Manager starts:
	`ERROR: java.lang.NullPointerException at org.apache.lucene.index.IndexReader.open`
	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:
	`arcsight searchindex -a create -m <manager-hostname> -u <admin-user-name> -p <password>`

47129	**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. Please ignore this information and continue with the installation or upgrade.
47206	During upgrade to ESM v5.0 GA, the *SSL Client Only* authentication option is selected by default. If you had set up your previous installation Manager to use *Password Based and SSL Client Based Authentication* method, the authentication method selected in the upgrade wizard panel will still default to *SSL Client Only*. **Workaround:** Make sure to change the authentication method back to **Password Based and SSL Client Based Authentication** during the upgrade.

Number	Description
51954 52680 52690 54003	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. **Workaround:** Please 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.
52394	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. **Workaround:** You can remove the unassigned `.art` files after an upgrade because they are duplicates. These `.art` files can be safely deleted.
52556	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. **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.
54344	Upgrades from ESM v4.0 SP3 or ESM v4.5 SP1 to ESM v5.0 on systems that include Solutions packages may result in the following warnings during the upgrade, or produce messages about invalid resources after upgrades (via a post-upgrade run of a "Resource Validation Report" or the arcsight resvalidate command). • Insider Threat Rule, Report, and Query: General Security – User Account Standard Violation **Workaround:** You can remove these resources before or after the upgrade. • Insider Threat Asset: webproxy.kaxy.com **Workaround:** Before or after upgrade, add the correct IP address for webproxy.kaxy.com • Any Solution Package: TRM – Quarantine rules **Workaround:** Either choose a valid TRM connector in the rule action, or remove these rules if you are not using them. This can be done before or after upgrade. • PCI Dashboard: AntiVirus Activity Overview **Workaround:** No workaround is necessary because the operation of the dashboard is not impacted If warnings related to these resources appear during the upgrade process, simply ignore these messages, or perform the suggested workarounds before upgrading.

Number	Description
55810	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. 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.
55935	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. **Workaround:** Cancel the installation after the Console is installed, and run the ArcSight Console Configuration Wizard to configure property settings. In <ARCSIGHT_HOME>/<Console_Build>/current/bin, run arcsight consolesetup at the command line. This way, SSL files are read and the Console can configure correctly.
61628	It is possible that on an upgraded system, the export of the some dashboards may fail with the following error. Invalid archive:Element type "X_COLUMN_NAME" must be declared. It usually impacts the dashboards that display the query viewer data. If that happens, add the following line at the end in the ARCSIGHT_HOME\schema\xml\archive\arcsight-archive.dtd file to make the export work: <!ELEMENT X_COLUMN_NAME ANY> Save the file then try to export again.
67378	During an upgrade from v4.0 SP3, there is a temporary condition where assets that are moved to different zones will be marked invalid, and you may see an error message that says something like [XXXX-XX-XX XX:XX:XX,XXX][ERROR][default.com.arcsight.common.persist.DeviceBrokerDelegate][populateLookupTableWithAssetData] Exception while adding asset data to the lookup table: [IP Address: 148.173.220.58 Mac Address: 00:00:00:00:00:00 Hostname 'phxipcarcagnt02' Zone ID: MP1Cv5fsAABCB5LYyFrIszg== Local ID: 17179869396] Ignore this message because the upgrade is still in process. As the upgrade completes, the assets are correctly rezoned.
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.
67547	After upgrading the Manager, you may see the following error in the server.logs file after running the Manager for a few days: Cannot allocate memory, not enough swap space. This happens when externally spawned processes have exceeded their allotted memory. In this case, search the logs for processes that are still running. These logs will include the recommendation to Please kill it manually.

Number	Description
67777	After uninstalling then re-installing the ArcSight Administration package, you will get invalid resources.
67797	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.
68075	During an upgrade to ESM 5.0 GA, autozoning will fail if the number of assets in a zone/group exceeds 1000. **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.
68098	Uninstalling and then re-installing the Global Variables package causes an exception. Since ArcSight Administration depends on this package, do not uninstall the Global Variables package.
68161	ESM Database installations on SUSE platforms: • 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**. • 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.
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.
68193	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.
68352	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.

ArcSight Database

Number	Description
50562	While uninstalling the ArcSight Database component that was installed by an administrator/root, if a non-privileged user (oracle user) uninstalls it, the uninstall link/shortcut does not get deleted.

Number	Description
56521	**On AIX only:** 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`. **Workaround:** • 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`.

ArcSight Manager

Number	Description
37959	In hierarchical ESM deployments, when you add lower level Managers to the setup, make sure that you do not use the system tables that were exported from an existing lower level Manager. One of the system tables contains a unique Manager ID. This Manager ID is used by the upper level Manager to make certain decisions when reaching back for base events for forwarded correlation events. If you use the exported system tables for the new Manager, the Manager ID of the existing Manager from which you exported the tables gets copied to the newly added Manager thus having two Managers in the setup with the same Manager ID. When two lower level Managers have the same Manager ID, the higher level Manager will pick a random lower level Manager, hence the results of the reach back may be unpredictable.
41582	Occasionally, when installing an exported package from a bundle file, you might receive the following error: `Install Failed: Resource in broker is newer than modified resource.` This error does not occur every time you attempt to install an exported package from a bundle. **Workaround:** Re-import the package.
42730	You cannot move an asset using Auto Zone if the asset is locked.

43678	If the search index file becomes corrupted, the Search index will be out-of-date and the following message appears in the Manager log:
	`[ERROR][default.com.arcsight.server.search.index.IndexResources][_init]`
	`java.io.IOException: read past EOF`
	Workaround: Regenerate the index by issuing the following command from the Manager <ARCSIGHT_HOME>/bin directory:
	`arcsight searchindex -a create`

53975	User is unable to set up sending pager notifications through the pager service provider. **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.

Number	Description
55969	**On Linux only:** You may experience high CPU utilization on the ESM Manager. This may be specific to your system/hardware. **Workaround:** If you are experiencing performance issues, try updating your drivers or reinstalling the Linux operating system.
56123	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. **Workaround:** Import the same package a second time.
57661	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. You therefore end up having two assets with the same hostname and dynamic address but different domain names.
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.
60808	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` and the Manager, having run out of memory, automatically restarts itself. **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.

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.

61524	For scheduled reports, when the “Run as” User's read and write privileges are taken away, the scheduled report is generated by the User who created the schedule (and not by the “Run as” User). If the “Run as” User has “read” privilege only, then the report is not generated.
62044	If you rename a resource which 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.
62109	Query viewers and channels display results from variable calculations differently. Query viewers and channels display results from variable calculations differently. For example, a value may be displayed as `-0.1` in a query viewer, and `-0.099999999999`... in a channel. This is due to the difference between how values with the data type double (floating point) are expressed in Java and Oracle. Not all fractions can be expressed precisely using the double (floating point) data type in Java. This results in a difference between data returned by SQL queries vs. in-memory operations.

Number	Description
62342	**On Windows only:** In order to run the NSS utilities on Windows, you are required to have the VC++ 2005 runtime libraries. If you plan to install ESM in FIPS or Suite B mode make sure that you have the .NET or vcredist_x86.exe installed on your machine before you install ESM: 1 Download vcredist_x86.exe from http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en 2 Install vcredist_x86.exe according to the instructions on http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en
63091	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. 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.
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`

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:
	`./arcdbutil sql username/password`
	`@../utilities/database/oracle/common/sql/runSessionListStats.sql`
	`exec runSessionStats`
	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.

<table>
<tr><th>Number</th><th>Description</th></tr>
<tr><td>66978</td><td>It is possible that during the actor import process from the Actor Model Import connector, one or more actor import files containing data for multiple actors may not have imported successfully into the Manager. This can happen because of network connection problems, an out-of-memory error, or some other problem that caused the import of that file to fail.

In such cases, ESM creates an archive file in <code>$ARCSIGHT_HOME/archive/webservices</code> for each actor import file that failed to import successfully. Each such archive file is created with the file extension '<code>.bad</code>.'

If an actor file did not import into ESM as expected, or as a matter of routine maintenance, you can check the <code>$ARCSIGHT_HOME/archive/webservices</code> directory for actor files that failed to import.

The <code>.bad</code> archive file contains all the missing actor information, and you can use the ArcSight Archive utility to import that file individually from a command line on the Manager system. For instructions about how to run the ArcSight Archive utility to import an archive file, see the topic "The Archive Command Tool" in the ArcSight ESM Administrator's Guide.

Notes:
• To see a list of commands available with the ArcSight Archive utility, include <code>-h</code> (for 'help') in the archive utility command script.
• If the archive file name starts with a dash (-), rename the file before running the ArcSight Archive utility to ensure that the command works.
• If the import process still produces errors that you are unsure about how to address, contact ArcSight Customer Support.</td></tr>
<tr><td>67328</td><td>Domain fields are set only in the context of a domain. Therefore, you must aggregate on the domain resource field while aggregating on domain fields to have the domain fields populated in the correlation event.</td></tr>
<tr><td>67790
67792</td><td>There is inconsistency in how variables are evaluated across resource channels:
1 In actor channels, variables are evaluated accordingly.
2 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.
3 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.</td></tr>
<tr><td>68173</td><td>When starting ESM Manager as a service on a Windows 2003 32-bit machine, the service cannot be started 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 <code><ARCSIGHT_HOME>/logs/default/server.std.log</code> file for the word "Ready." log message.</td></tr>
</table>

Number	Description
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`

68655	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:
	`... Search index utility completed: com.arcsight.tools.process.ProcessTimeoutException: Command did not finish in time.`
	Your searches may not return the expected results.
	Workaround: Regenerate the index by issuing the following command from the Manager's <ARCSIGHT_HOME>/bin directory: `arcsight searchindex -a create`
	If you have a large number of resources, you may run out of memory when running the above command, so make sure to set your memory equal to the heap size that you have set on the Manager. To do so,
	1 Set the ARCSIGHT_JVM_OPTIONS to the heap size of the Manager. For example:
	`export ARCSIGHT_JVM_OPTIONS="-Xms32m -Xmx3072m"`
	where 3072 is the max heap size set on the Manager.
	2 In the same command prompt window, run the searchindex command from the Manager's <ARCSIGHT_HOME>/bin directory:
	`arcsight searchindex -a create`

ArcSight Console

Number	Description
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.
60992	There is an issue with the ASIM connector payload using Wireshark as the external viewer. When the payload is retrieved in the Console, it is not correctly displayed in Wireshark. It is displayed correctly if the payload is first saved to an external file and then the file is viewed in Wireshark. **Workaround:** To view the payload, click the Save Payload button then save the payload to a local pcap file. Then open the file in Wireshark.

Number	Description
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.
35166	If you are running the sendlogs wizard and you click **Previous** or **Next**, an error message says `Error (Null)` **Workaround:** Cancel the wizard and start again.
36148	To search for resource IDs that begin with non-alphanumeric characters (such as the resource IDs for trends and queries), add double quotes around the ID. For example, to search for ^VVsOXg4BABCAIEuBhILMyg==, enter **"^VVsOXg4BABCAIEuBhILMyg=="** in the query text field.
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.
39407	The Scheduled Time column in the Scheduled Runs view covers both time ranges for runs that have already occurred and for runs that are pending. As a result, you will see some discrepancy in the time ranges shown in the column. For example, against the runs that have already occurred, you will see the lower end of the time range (For trends set to run hourly, if the time range is between 1:00 pm – 2:00 pm you will see 1:00 pm). The pending runs show the upper range (if the time range is between 1:00 pm – 2:00 pm you will see 2:00 pm). Trends that have already occurred will have a time difference that reflects the trend query schedule (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).
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.
49608	In a Hierarchy Map data monitor, after 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.
50968	If you delete an escalation-level notification resource, you receive the error "Group does not exist" in the `console.log` file. This error is incorrect and can be ignored.
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.
51094	**On Unix systems:** The drag-and-drop feature does not work in the Console. **Workaround:** Use the cut-and-paste feature instead.

Number	Description
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.)
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.
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:** Close a few channels as recommended by the error message.
56865	**On Linux only:** If you right-click on the port field in a channel and select Integration Commands->Portinfo, you will get an error. **Workaround:** Use the version in legacy tools.
57050	In the Query Editor, if you have read permission to a query but not to the global variables that are being used in the query, the resulting display will be incomplete. None of the global variable-related fields will be displayed. Also, you will not get an error saying that you are not able to view some resources in the query due to lack of sufficient permissions.
61659	When a user tries to modify a case while a case channel is open and an inline filter is applied, no data appears. **Workaround:** To successfully display available data, refresh the case channel.
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.

Number	Description
61931	When a filter is moved from one group to another and the data monitor that depends on that filter is packaged, exported, and re-imported on a different ESM installation, the data monitors may have missing filter attribute values. **Workaround:** Manually set the filter for these data monitors that are identified by the broken resource icon.
63460	Importing or exporting domain fields show these fields to be Unknown Fields in the rule editor. **Workaround:** To prevent this from happening, in the export and import, make sure to include the domain field set to which the domain field belongs.
64251	If you create an actor channel, add any new fields to the field set and not directly to the channel.
64333	Query viewers and channels display list results differently. Query viewers display lists the way reports do: one line per list entry while channels display lists the way data monitors do: `[entry1, entry2, entry3]`.
64334	Velocity-style expressions in local and global variables created or used on an actor schema are not supported.
64943	Copying and pasting are not supported only 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.
65421	Bulk deletion and import of actors are slow if category models are defined. **Workaround:** Create category models in the system after actors have been successfully imported in to the system.
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.
65708	The Console can become unresponsive if you are trying to access other resources while building category models with a large number of actors.
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.
66099	If you export a manual category model, the actors or groups in that category model are not included. There is no workaround.
66115	The category model graph can be inconsistent if a user-created actor field set is used in the category model and the field set has a local variable defined on either the parent field or the child field of the category model. For example, the category model is defined on Manager (parent field), and DN (child field) fields and the user-created field set has a local variable on the DN field.

Number	Description
66475	When running the Network Maps TRM command using the internal browser, an error message about one or more ActiveX controls is displayed. **Workaround:** Allow the browser to enable ActiveX controls.
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.
66665 67265	The Console's embedded browser is not supported on Red Hat Linux 5. **Workaround:** Use the external browser instead.
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.
66766	On a 64-bit Macintosh, displaying online help in the embedded browser is not supported. **Workaround:** Use an external browser instead.
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.
66925	Global variable fields will have no values if added directly to a channel. If added as part of a field set, the values are displayed.
67115	If you create a query on a field-based active list whose field names begin with **domain** (for example, domain1, domainfieldstring1, domainstr1), 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. **Workaround:** You should not create fields with names that begin with *domain*.
67195	After accepting the certificate from ESM Manager during the login process, i.e. first time this installation of the Console is connecting to the Manager, restart the Console for custom view dashboards to work properly.
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. If you experience issues due to name conflicts, change your custom cell names.

Number	Description
67348	If a domain field with an associated filter is deleted, and you re-create the field with the same name, it appears that you can successfully validate the filter. However, this domain field is seen on the Filter tab as an Unknown Field. This issue is seen in Rules as well. **Workaround:** To prevent this, re-create the domain field, associate it with the same domain field set, then validate the filter.
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.
67697	On the normal layout, Status text labels next to the icons are visible. On the custom layout, Status text labels may sometimes not be displayed. This is an intermittent problem that may be seen on the embedded browser and will go away once the data monitor is refreshed. **Workaround:** Wait for data to refresh or reload the custom view dashboard.
67798	**On Solaris only:** From the Console, support for web browser functionalities is limited to only viewing the online help in the external browser.
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.
67842	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. **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.
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.
67856	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. **Workaround:** Generate key pair for browsers and import the certificate into Manager's truststore, or copy the Console's key into the browser's keystore. See *ArcSight ESM Administrator's Guide* for details on how to do this.

Number	Description
67895	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.

67951	**On Macintosh platform only:**
	For existing ESM users, if your JRE was updated, you will see the following error when you try to log into the Console:
	`IOException: Keystore was tampered with or password was incorrect.`
	This happens because the Mac OS update changed the password for the cacerts file in the system's JRE.
	Workaround: Before you start the Console, change the default password for the `cacerts` file by setting it to the following in the `client.properties` file (create the file if it does not exist) in the Console's `\current\config` folder by adding:
	`ssl.truststore.password=changeme`

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 not supported on IE in 64-bit systems. **Workaround**: Use IE 32-bit version as your Console's external browser from the Console's Preference menu (Edit>Preferences>Program>Preferred Web Browser>External Browser). Then install Adobe Flash Player.
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. **Workaround:** 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.
68132	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. **Workaround**: Set LoggerPassword to Text type if you want to use the external browser for Logger commands. One issue with this workaround is that the password would appear as cleartext in your browser URL parameters.
68170	When used inside a filter, the `inActiveList` condition with a list parameter ignores the **All values must match** setting: even if that box is checked, the condition will match if any of the items in the list match. **Workaround:** The condition works correctly if used directly in a rule (instead of in a filter).
68478	When viewing image dashboards in an external browser and 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. This is a known issue. Click **No** to dismiss the message. You may also refresh the page.

Number	Description
64037 64742	When querying events with conditions on actor fields, SQL queries may run slow especially in the following cases: • List conditions are used. • Conditions on event fields are missing. In some cases, queries may even time out and not produce results.
67689 68154	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.
67876 68132	In the previous releases, color charts would display values with different colors even if the values belonged to the same series. In this release, the charts will use the same color for all values in a series. For example, if you are plotting successful and failed logins in a chart, successful logins as a series will have one color. Failed logins as another series will have a different color.
68291 45403	Embedded browser in Console is not supported on Linux 64-bit platform. **Workaround:** Use an external browser instead. You can set up the Console to use the external browser during installation.

ArcSight Web

Number	Description
25121	If you used a custom logo for ArcSight Web, the logo may not show up correctly when you upgrade ArcSight Web. **Workaround:** Update the logo manually after you upgrade ArcSight Web. See the ArcSight Web User's Guide for details on how to do this.
43702	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: (http://www.adobe.com/go/6b3af6c9).
46969	When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an active channel. This is a known issue.

<table>
<tr><th>Number</th><th>Description</th></tr>
<tr><td>52336</td><td>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 are not displayed properly and are virtually unreadable.

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.

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:
1 Log in to the ESM Console, choose Query Viewers in the Navigator, and right-click the Query Viewer you want to edit.
2 On the Query Viewer Editor, click to disable (uncheck) Use Default (if it is enabled), then enter a row limit of 100 or less.
3 Click Apply or OK to save the changes.</td></tr>
<tr><td>56258</td><td>When you create a case and you set the Estimated Restore Time, it is not updated with your changes.

Workaround: Define this setting on the Console. See the Console online Help for steps to do this.</td></tr>
<tr><td>63013</td><td>In ArcSight Web, there is no ability to define inline filtering on variables used in active channels.</td></tr>
<tr><td>64207</td><td>When adding correlated events to a case using ArcSight Web, your only option on the Edit panel is either to add to an existing case or create a new case. You have no option to include a base event.

Workaround: Use the Console for this task.</td></tr>
</table>

ArcSight Connectors

Number	Description
68697	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.

Analytics

<table>
<tr><th>Number</th><th>Description</th></tr>
<tr><td>40230</td><td>Sometimes after changing some the description on a trend, another trend depending on this trend may become invalid.

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.</td></tr>
<tr><td>51280</td><td>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:

<code>The query run failed because of the following reason:</code>

<code>com.arcsight.common.ArcSightException:</code>

<code>com.arcsight.common.introspection.queryable.QueryableFetchException:</code>

<code>Encountered persistence problem while fetching data: Unable to execute query: ORA-00979: not a GROUP BY expressionConditional variables in a SELECT statement with an aggregated field causes an Oracle exception (not a GROUP BY expression)</code>

Workaround:

1 Remove the ORDER BY fields in the Query resource.

2 Use the sort options provided by the Query Viewer or the Report.</td></tr>
<tr><td>53435</td><td>When you set the Schedule Frequency for a report, the Next Run Time field displays incorrectly in the Editor.

Even though the time displays incorrectly, the report runs at the time specified in the editor.</td></tr>
<tr><td>53484</td><td>Certain reports run for several hours and then time out or fail with the error message:

<code>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</code>

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 as well.

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.</td></tr>
</table>

Number	Description
54507	In Rules, the context menu option, **Verify Rule(s) with Events** (replay with rules), does not work for these types of active lists: • an event-based active list with values • a field-based active list with values, where all fields are mapped to event fields Verify Rule(s) 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.
55314	Variable names that contain dashes or hyphens (-) in the name 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: add (2.0,3.0). This rule will not trigger successfully, and the logs will show an exception indicating ESM is “unable to evaluate rule”. **Workaround:** As a best practice, do not use dashes or hyphens (-) in variable names. Underscores (_) are acceptable in variable names, but upper and lower case letters only are best.
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.
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.
59649	**Linux and Mac OS:** Logger integration commands are not available from the context menu on the Channels tab of the ArcSight Console. **Workaround:** To run Logger integration command for these operating systems, use an external browser.
63477	Scheduled rules using domain fields in their condition are not fired. **Workaround:** If you need scheduled rules to use domain fields in its conditions, set the property `turbo.enabled=false` in the Manager's `config/server.properties` file. By default, this property is set to turbo.enabled=true. Be aware that this will enable persistence of additional data fields if those fields are not being mapped into domain fields. This might have performance and storage impact in that scenario.

<table>
<tr><th>Number</th><th>Description</th></tr>
<tr><td>63709</td><td>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.
Workaround:
1 Create the CSV with the desired columns, for example: Name, Source Address, Destination Address.
2 Create a <code>schema.ini</code> file that has the following definitions for the CSV file:
<code>[yourfile.csv]
ColNameHeader=True
Format=CSVDelimited
Col1="Name" Char Width 255
Col2="Source Address" Char Width 255
Col3="Destination Address" Char Width 255</code>
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:
<code>[yourfile.csv]
ColNameHeader=True
Format=CSVDelimited
Col1=A DateTime
Col2=B Text Width 100
Col3=Col3=C Text Width 100
Col4=D Long
Col5=E Double</code>
For more information about the <code>schema.ini</code> file, perform an Internet search.</td></tr>
<tr><td>65477</td><td>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.</td></tr>
<tr><td>66801</td><td>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.</td></tr>
<tr><td>67210</td><td>After initially importing 50k Actors, you may experience sluggish performance in queries and channels. Performance improves after subsequent statistics collection.</td></tr>
</table>

<table>
<tr><th>Number</th><th>Description</th></tr>
<tr><td>67531</td><td>Category model is a beta feature of ArcSight ESM v5.0. Following are the requirements and limitations:
• Each category model requires 300 MB on ESM Manager. Viewing one category model at a time on ESM Console requires 1 GB heap.
• It is recommended that you view only one category model at a time on the Console.
• A category model in the system slows down actor imports; therefore, import actors prior to creating category model.
• Deletion of all actors is not recommended if category model is in the system.</td></tr>
<tr><td>67567</td><td>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.</td></tr>
<tr><td>68215</td><td>While editing a rule, if you activate any de-activated trigger, the Apply and OK buttons are not enabled.
Workaround: If the Apply and OK buttons are not enabled, edit a field on any tab. For example, go to the Attributes tab, select the Description field, and enter a space at the end. You can apply this workaround on any field on any tab without changing your original content.</td></tr>
<tr><td>68262</td><td>If you set "NSPAuth" as Password type and run TRM commands in the external browser, you will be redirected to the Login page.
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.</td></tr>
<tr><td>66128
66129</td><td>The newly introduced category model function <code>HasRelationship</code> 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.
If your query uses a global or local variable with function <code>HasRelationship</code>, 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 <code>HasRelationship</code> is useful for the evaluation of conditions rather than as a selection column for queries.</td></tr>
<tr><td>63732</td><td>If your zone names have commas (for example, abc, inc.) and the connector tries to populate the zone-related fields on the connector, an error is generated in <code>agent.log</code>. The error includes the following string:
... <code>Expected 4 tokens and got 5:</code> ...
Workaround: Avoid using commas in zone names.</td></tr>
</table>

Localization

Number	Description
43313	All localized languages: If you add a column to a channel and add an inline filter, you will see an error dialog. An INVALID name is given for the stage. The contents of this error dialog will appear in English and will not be translated.
43316	All localized languages: The following field values will appear in English (they are not translated): • Trend Partition Size • Partition Retention Period • Imported Trend Start Time • Imported Trend End Time
43366	When the Workflow package is installed on a localized version of the Manager, exceptions will be present in the server.log. These exceptions occur because certain aspects of the Cases have not been localized for this release of ESM.

Issues Fixed in v5.0 GA

The following issues were addressed in this release.

Install and Uninstall

Number	Description
46995	Fixed an issue where in Console mode, the installer sometimes did not validate the Uninstall Links folder. The system successfully validated the Base folder, but without user write permissions it did not create an uninstall link.
55853	The ArcSight Database installer did not include error checking or validation per Oracle supported schema user naming conventions. If the user names specified contained anything other than alphanumeric characters, the ArcSight Database installer would prevent create/recreate of the schema and display the following error code: `error ORA-00921: unexpected end of sql command` For ArcSight Database install and schema setup, please keep in mind that Oracle supports only alphanumeric characters for database user names, and will not accept a dash (-) or underscore (_) in these names.

Upgrade

Number	Description
61714	**On Unix only:** When upgrading from ESM 4.5 SP1 Patch 2/Patch 3, to ESM 4.5 SP2, the dbcheck script produced an error. This issue has been fixed in this release.
62801	Fixed an issue when upgrading from ESM 4.5SP1/ESM 4.5 SP1 Patch1/Patch 2/Patch 3, to ESM 4.5 SP2, customized shortcut keys disappeared from the Console UI.

ArcSight Database

Number	Description
33137	When creating system tables, you received error messages indicating that a column subtype is not a string. These errors are informational only and may be ignored.
57116	**On the Solaris platform:** Occasionally, the following error displayed when you tried to create a database instance. `Database test connection failed. ORA-07445: exception encountered: core dump [kgskhighthreshold()+72] [SIGSEGV]` This is due to an issue described in Oracle ticket number `Doc ID 805206.1`. If you encounter this error, contact ArcSight Customer Support for assistance.

ArcSight Manager

Number	Description
17714	When a non-admin user runs a report, the report shows assets and cases even though a non-admin user does not have the rights to view the assets or cases. It has been determined that the behavior described is expected. Only event-based filters apply to event reports and queries. So, if an event that the user has access, includes a resource (Asset etc.), users will be able to see the fields of the resource that are part of the event schema in the context of that event.
30009	Inconsistent use of uppercase and lowercase letters in the field data in the main event table resulted in slow database performance and sometimes led to errors. The UI now enforces case-sensitive content.
31027	If synchronizing with LDAP for authentication, dots and commas inside usernames are now supported. Examples are `user.name` and `name,user`.
36553	**Windows only:** The command line tools `arcsight managersvc start` and `arcsight managersvc stop` are now supported in ESM v5.0.

Number	Description
44306 44309	Several fixes were introduced to the SetEventField action for a rule: • You can now enable the option to enter multiple lines of text. • The OK, Cancel, and Help buttons are displayed in the edit text box. • The help link now opens the correct Help file.
45376	Internal events can now be blocked from being persisted in the database, regardless of event type.
46488	Events going through the event flow occasionally did not have event IDs.
49076	Disabled rules sometimes threw exceptions.
50794	In a hierarchical Manager setup, the base events for only some of the correlation events get forwarded to the upper level Manager, and this behavior is not predictable. If the upper level Manager needs the base events for these correlation events, and the base events are not present on the upper Manager, the base events get fetched on-demand when the user opens the correlation event in the event inspector panel on the upper level Manager. It has been determined that the behavior described is expected.
56466	Fixed an issue where Pattern Discovery caused some unnecessary full garbage collection cycles on the Java Virtual Machine (JVM). This was done to ensure support for memory usage required by large data sets.
56556	There is no way to specify a NULL value for “preview” input to a Variable function on the Console Common Conditions Editor (CCE). The Preview assumes that a blank field for an input is an empty string. Therefore, you cannot use the Preview function on the Variable dialog to test inputs for a parameter with NULL values. It has been determined that the behavior described is expected.
57622	Fixed an issue where you did not see any audit events generated when a resource was locked. This issue is resolved. Audit events get generated on locking the resources now.
60382 60383	The '/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/External Source' filter in ESM has been modified as follows: ((NotMatchesFilter("Internal Source") AND (Attacker Zone ID Is NOT NULL OR Attacker Asset ID Is NOT NULL))
60690	Fixed an issue with trend data viewers when applying a filter on the device direction field, no data returned and an exception was logged in the server.log file.
67847 51493	The export function could only export an entire table, but could not export selected events. This issue has now been fixed and you can now export selected events.

ArcSight Console

Number	Description
20602	Inside a case there was a Delete option to delete the actions history under Notes. To prevent users from deleting a case, the Delete option on the context menu for historical notes is available only if the resource is not a case.
24496	Drill down from Event Graph data monitors to channels are now supported when the Event Graph data monitor uses Variables to retrieve or parse event information.
35622	If a channel was undocked, the recalculation of field widths was inconsistent. Only the last field was expanded across the additional space. That is the default behavior, but users can now specify a preference for resizing all columns. In the `ARCSIGHT_HOME/config/console.properties` file, change the `console.ui.views.AlertSortTable.autoResize` from false to **true**.
35766	Previously, when creating a query, the editor portion on the Console did not provide enough space for the drop-down menu to be visible to the user. The UI was changed to fix this issue.
38832	When you displayed Assets in an Asset Channel, the Device Zone Network Name column did not get populated in the Grid view. To view the details of an Asset, click the right-facing arrow in the first column to open the **Asset Detail** box.
40929 42409	Locations expressed in longitude and latitude (with degrees and seconds) are now correctly saved.
41305	When a custom column in an Active Channel used the "$fieldname notation", you would see the "$fieldname" value in the cell if the value of the field was null. This issue has been fixed in this release.
43458	Trends can now populate an active list. After saving a new trend, the Actions tab is enabled.
43466	In the previous release, the Console's Sendlogs feature generated duplicate error entries for Manager logs. This issue is no longer reproducible in ESM v5.0.
49105	Fixed an issue where the Active Channel did not get updated after the events were annotated.
52617	Fixed an issue where the Active Channel "Slide Show" feature (View > Slide Show > Start) maximized the viewer to full screen and took over the entire screen space. If you were working on multiple monitors, the slide show would take over your primary display.
56556 56557	There is no way to specify a NULL value for "preview" input to a Variable function on the Console Common Conditions Editor (CCE). The Preview assumes that a blank field for an input is an empty string. Therefore, you cannot use the Preview function on the Variable dialog to test inputs for a parameter with NULL values. It has been determined that the behavior described is expected.

Number	Description
61713	On ESM 4.5 SP1, if the "\" character was used on a rule condition, the rule failed to compile. An error message appeared. v4.0 SP3 did not have this problem. As a result, if you performed an upgrade from 4.0 SP3 to 4.5, all the rules that have "\" in the their conditions were broken. This issue has now been fixed and you can use the "\" character on a rule condition in v5.0.
62276	When adding a column to sort on in a channel, it no longer auto-saves the criteria for the channel if you select No in the Save Changes dialog.
62370	Fixed an issue where you couldn't filter a channel with a condition that contained the '@' character. Not escaping the '@' character in the filter condition seemed to introduce additional unexpected characters into the condition text. Escaping the '@' character with a backslash avoided the unexpected characters but the filter had no effect. You can now enter "Name contains '@'" and the UI won't insert a parameter for you, unless you are inside the Query Editor.
65282	If columns were moved in the active channel the sort on the channel in the new location would sort the field that was originally in that location. This issue has been fixed in this release.
67935	Fixed an issue where the search for the reference page for "snort" would result in a "500 error".

ArcSight Web

Number	Description
24404	Fixed an issue in ArcSight Web where channels with conditions that referred to an Event field that ends in `Resource` would fail. ArcSight Web now supports the use of these fields as a filter condition.
43327	Fixed an issue where ArcSight Web channels did not support sorting by a time field other than the one chosen as the channel time stamp. For example, a channel in ArcSight Web could not use Manager Receipt Time as the timestamp and End Time as the sorting timestamp. Attempting to use such a channel in ArcSight Web produced an error.

DST Issues

Number	Description
54713	If you had scheduled a report to run every two hours before the start of Daylight Saving Time and scheduled the first run to occur at an even numbered hour (for example 2:00 pm), once DST begins, the scheduled run for this report would occur on odd numbered hours (for example 1:00 am, 3:00 am, etc.). The interval will continue to be every 2 hours. This issue is now fixed.

Number	Description
54749 55835	Depending on your time zone, you might have seen your scheduled tasks running off by 15 minutes to an hour. For example, scheduled tasks would run 15 minutes early in America/Guyana, whereas in Asia/Bahrain or Europe/London it would run one hour early, etc. This has now been fixed and your scheduled tasks will run on time.
55207	Daily Trends (only existing trends) were out of sync by one hour after the October 2008 DST change. The query interval should be set manually to reflect the correct times for existing trends. For assistance in setting the query interval manually, contact ArcSight Customer Support.

Analytics

Number	Description
24280	The report editor no longer opens on a highlighted report if you are only expanding a report group.
24027	Fixed an issue where if temporary reports were automatically removed from the user's personal report archive folder because expiration time is reached, the folders were also removed.
25873	An old problem about the knowledge base not allowing spaces in the path when importing a new article is no longer reproducible in ESM v5.0.
38832	Fixed an issue when you displayed Assets in an Asset Channel, the Device Zone Network Name column did not get populated in the Grid view.
39932	When applying a new channel to verify rules, occasionally the generated events would not show up in the channel correctly because the correlated events didn't match the filter. This issue has now been fixed.
44029	In v5.0, if you change the property, console.ui.reports.expString=$Now+1M in user.ast file, the change will be applied **only** to reports created after you changed the property. Any existing reports will not see the change. In previous releases, this behavior was not consistent across all reports.
44032	In v5.0, if you change the value of the console.ui.report.email_format property in the user.ast file, the change will take effect **only** for new reports created after the change.
45569	Reports now match the format provided in the template.
47979	The following fixes were introduced in reports: • Through the Alias field, you can use meaningful field names in reports. • Custom parameters defined in the query are applied to the report. • If you go back to the query and add columns, the report will show the changes.
50174	Fixed an issue when you changed and saved some values in a query, all reports parameters related to graphs and tables that were saved when the report was open in the Inspect/Edit tab at the same time, were removed. However, if you closed and re-opened the report, you would find the report parameters that were saved remain saved.

Number	Description
53206	/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Notify on Successful Attack looks for base and correlation events with a high or very high priority and a Device Event Category of /Attack/Success, unless the attacker information is in the Trusted List (for vulnerability scanners, etc.). This bug was reported because it was misfiring under conditions where it should not have fired. The correlation event was actually generated from /All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/Probable Successful Attack – DoS, which was changed to require a different attacker for the two base events (it is a join rule), and increased the aggregation count to 3 events within 2 minutes.
56263	Fixed an issue when copying a report that had a scheduled job associated with it, the job was transferred to the copied resource but it didn't get displayed as a job
57392	The HTML report settings have been enhanced in v5.0 such that while creating the report in HTML, you now have the option to turn off the header and pagination by setting the following property in `server.properties` file: `report.pagination=true`
58481	Fixed an issue whereby some reports running under separate process fails with message 'java.io.FileNotFoundException'.
58490	The old Device Licensing reports have been deprecated. The newly created reports for v5.0 are located in /All Reports/ArcSight Administration/ESM/Licensing folder.
63545	Fixed an issue where after applying a non-default border style to a table, for example, if you changed the border style to say, ultra thin line for a column which is set to page break then the border style was enforced but the page break no longer worked.

Documentation

Number	Description
24954	The Console online Help and User Guide now explain the discrepancy between reports from a scanner and reports from the asset editors. Reports from the asset editors will include both scanner data and vulnerability mappings stored in the ESM system.
25002	If you receive an error saying that you cannot save the keystore if the keystore type is of PKCS #12, it is because your password needs to be four characters or less. This has now been documented in the *ESM Installation and Configuration Guide*.
40391	The ESM User's Guide for v5.0 documents the available functionality on the image dashboard.
56271	The Trends audit events are now documented in the ESM User's Guide and Console Online Help under Reference Guide > Audit Events > Trends topic.
56707 56709	In previous releases the PKCS #11 documentation was a part of the installation documentation for the various ESM components. This used cause confusion. For v5.0, the PKCS #11 related documentation has been moved to a separate appendix in the ESM Installation and Configuration Guide. This appendix is titled Using PKCS #11 Token.
58679	The topic in ESM Console Help > ESM User's Guide > Case Management and Queries > Managing Cases has been enhanced to include information on the fact that events associated with cases, get archived off based on retention policy.