Release Notes

ArcSight Express™ v3.0
Featuring ESM with CORR-Engine

August 2011

ArcSight™
An HP Company

Release Notes ,
ArcSight Express™ v3.0

Revision History

Date	Product Version	Description
04/06/2012	ArcSight Express™ v3.0	Added ESM-49830 to the Open Issues section and updated the Contact Information section below
08/31/2011	ArcSight Express™ v3.0	Release Notes for ArcSight Express™ v3.0

Contact Information

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

Contents

ArcSight Express™ v3.0 1

Welcome to ArcSight Express™ v3.0 1
Release Contents 1
Installation and Configuration 1
ArcSight ESM Console 2
ArcSight Forwarding Connector 2
Threat Response Manager (TRM) Support 2
Usage Notes 2
Loading Dashboards 2
About an Adobe Flash Player Limitation 2
SSL Support for the Management Console 2
Supported Scripts 3
Geographical Information Update 3
Vulnerability Updates 3
Open Issues in ArcSight Express v3.0 4
Analytics 4
ArcSight Console 7
ArcSight Manager 11
ArcSight Web 14
CORR-Engine 14
Connectors 15
Installation and Upgrade 15
Management Console 15
Pattern Discovery 17

ArcSight Express™ v3.0

Welcome to ArcSight Express™ v3.0

ArcSight introduces ArcSight Express v3.0 with the Correlation Optimized Retention and Retrieval Engine (CORR-Engine), a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches. This provides a number of benefits, including increased performance and more compact data storage.

Release Contents

ArcSight Express v3.0 includes the following software components:

- ESM version 5.1.0.1281.3(BE1281)
- CORR-Engine version BL1093
- Process Management version 1.0-1117

Installation and Configuration

For detailed installation and setup instructions, refer to Getting Started with ArcSight Express, included with your ArcSight Express shipment.

After you have set up the appliance successfully, you will need to configure it. The First Boot Wizard guides you through the setup and configuration of the operating system and the components that reside on the appliance. It prompts you to configure the Red Hat Enterprise Linux operating system first and then the ArcSight Express software components (the Manager and the CORR-Engine). For help on the wizard panels, refer to the Configuration Guide, which you can download from the ArcSight Customer Support download site.

ArcSight Express appliance contains the following components.

- **Manager** provides correlation and analytics. It manages, cross-correlates, filters, and processes all security-events in your enterprise. The ArcSight Manager includes a Correlation Engine, Connector Data Manager, tracking and resolution functions, and analytics and reporting capabilities. The ArcSight Manager uses a database to store events and security monitoring content.
- **CORR-Engine** is a proprietary data storage and retrieval framework that receives and processes events at high rates and performs high-speed searches. It also saves configuration information, such as system users, groups, and permissions and defined rules, zones, assets, and reports.
- **Management Console** provides a streamlined interface for managing users, storage, event data, and monitoring events. It includes ArcSight Web which is the web interface

to the Manager for operators and analysts engaged in network perimeter and security monitoring.

ArcSight ESM Console

Install the ArcSight ESM Console separately on a system other than the ArcSight Express appliance. You can download the Console installer from the ArcSight Customer Support download site. For instructions on installing the Console, refer to the Configuration Guide.

Console Supported Version

This release of the product supports the ArcSight Console version 5.1.0.1281.3. You can download and install one of the following depending on your platform:

- ArcSight-5.1.0.1281.3-Console-Win.exe
- ArcSight-5.1.0.1281.3-Console-Linux.bin
- ArcSight-5.1.0.1281.3-Console-MacOSX.zip

ArcSight Forwarding Connector

ArcSight Express v3.0 supports Forwarding Connector version 5.1.2.5857. Install and configure the Forwarding Connector separately after you have configured the appliance using the First Boot Wizard. You can download its installer from the ArcSight Customer Support download site. For instructions on configuring the Forwarding Connector, see the Forwarding Connector User's Guide, which you can download from the ArcSight Customer Support download site.

The Correlated Event Forwarding Connector (CFC) is not supported with ArcSight Express v3.0. Please use the version of the Forwarding Connector mentioned above.

Threat Response Manager (TRM) Support

The minimum supported version of TRM with ArcSight Express v3.0 is TRM v5.0.

Usage Notes

Loading Dashboards

Before you load a Dashboard in ArcSight Console or the Management Console, make sure that Adobe Flash Player 10 is installed on the system from which you will be running the ArcSight Console or the Management Console. Dashboards will not load correctly if Adobe Flash Player is not installed.

About an Adobe Flash Player Limitation

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).

SSL Support for the Management Console

The Management Console does not support SSL Client Authentication for this release. Please use Password Based Authentication instead.

Supported Scripts

See the Administrator's Guide for a list of supported scripts. Running unsupported scripts on the appliance may produce unexpected results, including system failure or data loss.

If you inadvertently run unsupported scripts, rebooting the system will restore proper operation in most cases.

Geographical Information Update

ArcSight Express contains recent geographical information used in graphic displays. The version is GeoIP-532_20110601. Refer to the ArcSight Context Update Release Notes dated June 2011 for more information.

Vulnerability Updates

This release of ArcSight Express includes recent vulnerability mappings (June 2011 Context Update). Refer to the ArcSight Context Update Release Notes for the vulnerability updates.

Open Issues in ArcSight Express v3.0

This release contains the following open issues. Use the workarounds, where available.

Analytics

Issue	Description
ESM-47679	Currently, for Data Monitors that provide the ability to GroupBy specific fields, you can group by any Customer related fields such as Customer Name, Customer URI, etc. All these options should be disabled except for the Customer Resource.
ESM-47360	In the Attributes panel of the ActiveList editor, the Optimize Data checkbox is unchecked by default. When you check this checkbox, it makes the active list use the Optimize Data feature, but you cannot delete the entry in the active list.
ESM-46869	When using the RequestUrlHost as a field in a Trend, the length of the column created is 64 characters. This is too short and does not match the length of similar fields in the event, such as Target Hostname and Source Hostname which are currently 1023 characters.
ESM-46632	On the Rule Editor's Aggregation Tab, if you select the Add button and then click Help, it opens the wrong help topic. To find the correct topic, scroll the Help topic Contents list on the left to Rules Authoring > Specifying Rule Thresholds and Aggregation > Setting or Changing Rule Thresholds.
ESM-46530	When an InActiveList condition is used directly in a Query it gets only the matching row. But, when used in a Filter first and the Filter is added into the Query, additional rows get returned.
ESM-40449 TTP#66622	When exporting events from the Case Details channel, archived events do not get exported.
ESM-39856 TTP#65477	If you use the embedded browser in Windows to view a report, the report may not appear until you resize the panel. Workaround: Resize the panel before running a report. You may want to try several resizings to get the desired results.
ESM-39632 TTP#64943	Copying and pasting are not supported for conditions with variables. For example, if you create a filter for an active channel and used the Common Conditions Editor to add condition statements, copying and pasting into another editor (for example, a Rule editor) may result in an error. Workaround: Manually re-enter the conditions.
ESM-38702 TTP#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. Workaround: To prevent accidental removal of a top-level group, as in the case of All Actors, create a group under it and add a number of actors to this group. Then add this group to a package. In this case, if you remove this package, you only remove the associated groups and resources in that package.
ESM-38286 TTP#62366	Cyrillic (Russian) characters are not displayed correctly in emails when emailing reports. Workaround: Set the property email.charset.encoding.default=UTF-8 in the server.properties file for it to work.

Issue	Description
ESM-38079 TTP#62044	If you rename a resource that has dependent resources, do not re-use the deleted resource's name when creating another resource of the same type because the dependent resources may refer to the new resource with the old name.
ESM-37810 TTP#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.
ESM-35381 TTP#55314	Variable names that contain hyphens (-) do not work properly when included on the right side of a comparison in a condition statement. For example, consider a rule with a condition that compares the JME argument sqrt(4) to a variable named abc-cde, where the value of abc-cde is: 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: Do not use hyphens (-) in variable names. Preferably use upper and lower case letters only, although you can use underscores (_) too.
ESM-35070 TTP#54507	Verify Rules with Events (replay with rules) does not work for the following 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 Rules with Events does work for other types of active lists. Also, valid active lists work properly with real-time rules when they are deployed, including the two types of active lists described above.
ESM-29633 TTP#40230	Occasionally, after changing a trend's description, another trend that depends on this trend may become invalid. Workaround: You can usually re-enable a trend that was incorrectly disabled by making any minor change on the trend (For example, you could toggle the trend's enabled state off and then back on) and then saving it. This will force the re-validation of the trend and re-enable the trend.
ESM-29348 TTP#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 (for example, one hour for hourly queries), while the pending runs will have a time difference that reflects the overall task schedule (for example, 24 hours if run once a day).
ESM-26488 TTP#33835	If you import the content of an older package into an existing newer package, the contents from the two packages get merged. The resulting package will consist of contents from both packages. The relationships will be merged, but the attributes will be picked up from the old package. Workaround: Export the new package to a bundle file so that you can recover it if need be. Then delete the new package before you import the old one.

Issue	Description
NGS-1846	In the Console, EPS license compliance will be enforced on the following viewers. - channels (event and resource channels) - data monitors - query viewers and query viewers in dashboard - pattern mining (Creating new snapshot. You should be able to view existing snapshot) - event graph from channel - geo graph from channel - category model view - image dashboards on Console and ArcSight Web (not the Management UI) While viewing any of the above in the Console, if you exceed the License limit threshold, the existing viewers remain undisturbed but if you create a new viewer or stop a channel and replay it then you will see an error. In ArcSight Web, only channels and dashboard viewers are affected.
NGS-1835	During the punitive action period of the EPS License violation, there are two issues related to data monitors: 1. For any existing data monitors, when you try to edit them (right-click and select Edit data monitor), a NullPointerException error dialog is thrown. After the punitive action ends, the data monitor can be edited without any exception. An error message window pops up with NullPointerException and the exception is displayed in the Console stdout 2. When a new data monitor is created, it brings up the editor. After you select a type of data monitor, the editor does not populate the values to be input for the type of data monitor selected and you see an exception in the Console stdout. Workaround: These issues can be safely ignored because during an EPS License violation the data monitors will not show any data.
NGS-1517	Active Channels will show no matching events to the users of a custom group in the absence of an enforced event filter specified for that group. This behavior in the Active Channels is not consistent with the behavior in Query Viewers and Reports.
NGS-1059	Long running reports and replay of large number of events with rules might impact event throughput. Try to limit long running report/replay rules or run them during an off-peak time.
NGS-448	In some cases, a query may run for more than 10 hours (but less than 20 hours) before being canceled. If you launch a query that does not end in a reasonable amount of time, you can do one of the following: - Cancel the query. A number of resources (such as Reports, Trends, Query Viewers) have ways to cancel a query or impose time limits. - If this does not work, you could use the MySQL command line to "kill" the query's thread. - As a last resort, you can restart the Manager to cancel such a query.

ArcSight Console

Issue	Description
ESM-46633	The Help window for Rules is inactive. This is seen while you define a Set Event Field action. Workaround: Click Cancel or OK in the Set Event Field window. This will allow you to see the help information. After reading the help, you can resume entering the settings in the Set Event Field.
ESM-46629	On the Mac OS X with Safari as the default browser, you cannot access the context sensitive help. When you click the Help button to display the context sensitive help for the topic, the browser displays a blank page. This is a known behavior in Safari if/when there is more than one # character in the URL. The URLs to the Help pages contain multiple # symbols. Workaround: Use Firefox instead of Safari as the default browser. To use Safari, after the Help page loads, use the Contents tab to select the desired topic or use the Search tab to search for specific topics.
ESM-46226	The GetGroupOfAsset variable function does not return results in SQL mode (in conditions for reports, query viewers, Pattern Discovery, active channels).
ESM-41641 TTP#69565	On Macintosh only: If you open a channel, select some rows, right-click on them and select Print Selected Rows from the resulting menu, it causes the Console to crash. Workaround: Before you start the Console, make sure to set up a default printer to which to print. This problem occurs when you do not have a printer set up.
ESM-41344 TTP#68478	When viewing image dashboards in an external browser, if you keep the dashboard running, you will get an error saying that a script on the page is causing the browser to run slowly and if it continues to run, your computer may become unresponsive. This error appears after every few hours while the image dashboard is running. Workaround: Click No to dismiss the message. You may also refresh the page.
ESM-41116 TTP#68018	After creating a statistics data monitor, adding it to the dashboard, and switching to custom view mode, the dashboard does not get launched. This happens on the external Internet Explorer (IE) browser on a 64-bit Windows platform. This is because Adobe Flash Player is required but is not supported on IE on 64-bit systems.
ESM-40943 TTP#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.
ESM-40935 TTP#67689	On a Windows Vista 64-bit system, charts cannot be viewed in custom view dashboards when using Internet Explorer (IE) as the external browser. Workaround: Use the 32-bit browser, such as 32-bit version of IE or Mozilla Firefox, and also download Adobe Flash Player.
ESM-40917 TTP#67652	If you delete a large number of actors through the ESM Console, the Console may become temporarily unusable. However, the Manager will continue processing in the background and updates the database with your changes. Once 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 Customer Support for assistance in detecting and cleaning up this condition if you suspect it has occurred.

Issue	Description
ESM-40739 TTP#67195	The very first time that you start the Console, you must restart the Console after accepting the Manager's certificate in the popup. This is required in order for the Custom View dashboards to work properly.
ESM-40587 TTP#66906	Correlation events may occur before the base event that triggered the correlation event in channels sorted by time. This happens if the event end time for the correlation event is the same as that for the base event. Workaround: Add a sort column in the channel to sort events, first by end time, and second by type of event. Base event type is 0 and correlation event type is 1.
ESM-40514 TTP#66766	On a 64-bit Macintosh, displaying online help in the embedded browser is not supported. Workaround: Use an external browser instead.
ESM-40506 TTP#66753	On the Macintosh platform, setting Safari as the preferred external browser using the Console's Preference menu (Edit>Preferences>Program) will result in the wrong URL. Workaround: Change the setting from the Console's Preference menu (Edit > Preferences > Program > Preferred Web Browser > External Browser) to open. Next, make sure Safari is the default browser in your Mac OS(Safari > Preference > General > Default) web browser.
ESM-39980 TTP#65708	The Console can become unresponsive if you are trying to access other resources while building category models with a large number of actors.
ESM-39829 TTP#65421	When there are category models in ESM, deleting actors will require these category models to be re-built. Each rebuild may take seconds. In case thousands of actors are deleted, the whole deletion period may last for hours because actor deletion launches a category model rebuild.
ESM-39331 TTP#64251	If you create an Actor channel, add any new fields to the field set being used by the channel instead of directly to the channel.
ESM-38961 TTP#63568	For image view mode, when a background file is uploaded, the Console does not provide an option for a location. The file automatically goes into your personal folder. Workaround: After the upload, move the file to a preferred folder.
ESM-38014 TTP#61931	When a filter is moved from one group to another and data monitors that depend on that filter are packaged, exported, and re-imported on a different ESM installation, the data monitors may lose some filter attribute values. Workaround: Manually set the filter for such data monitors that are identified by the broken resource icon.
ESM-37868 TTP#61659	When you 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.
ESM-37344 TTP#60500	On a Manager when a large number of cases reside in a single group, you can't pick a case for "Add to Existing Case" rule action in the Rule editor. This is because the resource selector only shows leaf nodes when there are less than 1000 cases in a group. This happens for all resources. Workaround: Make the resource hierarchy less flat so that there are no more than 1000 resources in a single group.
ESM-36154 TTP#57290	In the ESM Console, if you associate multiple knowledge base articles to a resource, you have to go through a popup menu to choose which article to open. This popup menu will appear to be free floating - it doesn't appear near the resource you just right clicked on.

Issue	Description
ESM-36055 TTP#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.
ESM-35998 TTP#56865	On Linux only: If you right-click on the port field in a channel and select Integration Commands > Portinfo (Linux), you will get an error.
ESM-35465 TTP#55476	If you open 10 channels and view them, then delete these 10 channels from the resource tree, you will not be able to open any more channels. You will see the following error: "Unable to create communication mode with server: The maximum number of open event channels (10) has been exceeded. Please close one or more individual event channels to continue." Workaround: Restart the Console.
ESM-33453 TTP#51094	On Unix systems: The drag-and-drop feature does not work on the Console. Workaround: Use the cut-and-paste feature instead.
ESM-33440 TTP#51072	If you right-click on a block in a Hierarchy Map Data Monitor and select Show Events, no events are returned if variables are present in the Source Node Identifier.
ESM-32705 TTP#49608	In a Hierarchy Map Data Monitor, once a color range is specified, you cannot change the color mappings on the range. Workaround: Delete the existing color mapping and create a new one with the color mapping of your choice.
ESM-31127 TTP#45403	On the Linux 64-bit platform, the Console does not support an embedded browser. Workaround: Use an external browser instead. You can set up the Console to use the external browser during installation.
ESM-28890 TTP#38270	While installing a package, if you cancel the installation before it is completed, the Import button is disabled. Workaround: Refresh the Console or log in to the Console again to enable this button.
ESM-27970 TTP#36148	To search for Resource IDs that begin with non-alphanumeric characters (such as the Resource IDs for Trends and Queries), enclose the ID in double quotes. For example, to search for ^VVsOXg4BABCAIEuBhILMyg== Enter "^VVsOXg4BABCAIEuBhILMyg==" in the query text field.
NGS-1830	If your Macintosh machine automatically updates the JVM to version 1.6.0_26 you could encounter a Console login failure which throws the following exception: com.arcsight.common.ArcSightException: Could not initialize SSL Client. Workaround: Copy the old cacerts file from the previous JVM installation that existed on your machine before the update and place it in the most recent JVM location. Since Mac OS X does not keep the old copies of the JVM, it is a good idea to back up the current JVM in order to preserve the cacerts file. The cacerts file is located via the symbolic link: /System/library/Java/JavaVirtualMachines/1.6.0_jdk/Contents/Home/lib/security, which points to /System/Library/Java/Support/CoreDeploy.bundle/Contents/Home/lib/security.

Issue	Description
NGS-1795	On non-Windows platforms, when you view dashboards with Custom layout option in the Console, you get an error, "Failed to create embedded browser, launching external browser"
NGS-1747	On Linux systems, when viewing dashboards, if you select the Investigate option you will see duplicate menus.
NGS-1401	The Actor Change Log Dashboard won't show any data for the Actor Change Log Data Monitor if any row in the Data Monitor has missing priority value.
NGS-1262	If a dashboard contains a Query Viewer that has a large row limit, the Console may hang while loading this dashboard in Custom Layout view. It is a good practice to keep the row limit of Query Viewers to less than 100 before viewing the dashboard in custom layout format.
NGS-146	This issue affects all event-based Active Channels (ACs) that include InCase filtering condition. Such ACs will not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit. The chances of this issue happening is relatively low because the CORR-Engine provides powerful event compression and it can support very long retention periods given sufficient disk space.This reduces the chance of events expiring while bound to an open case.

ArcSight Manager

Issue	Description
ESM-49830	In a hierarchical ESM deployment where you have source Managers and destination Managers, the destination Manager will occasionally misidentify the forwarded event when the event is forwarded from source to destination. This will result in an Event ID that could be a duplicate of an existing event in the database on the destination Manager, or result in an Event ID that will soon be a duplicate of a future Event ID. In either case, the end result will be local and remote events with duplicate Event IDs. This might impact the retrieval of base events from the source Manager.
ESM-47526	Asset creation for assets with similar hostnames but different domain names get resolved as duplicate because of which while importing assets using the Network Import Tool or Asset Import Connector, all assets do not get created. This happens if two or more assets have the same hostname even if the domain names are different. The default behavior should be to check the domain and hostname parts to create an asset. Workaround: Set the asset.lookup.hostname.resolve.without.domain property to false in the server.defaults.property file.
ESM-47471	The name of the customer was incorrectly set for ArcSight Internal Events if the customer had rules or Data Monitors that aggregate on only a few customer related fields rather than aggregating on all customer related fields.
ESM-47363	If the customer name contained the special character '&' in the OI (organization group(s)) the group did not get processed when translated to a URI. This created an xml.bad file in the manager/archive/webservice directory. When this happened, it prevented any Actor from getting created in the List.
ESM-47152	If you hada case channel being sorted on an integer field, for example Display ID, if you created a new case, you got an error similar to the following: ArcSightRuntimeException: java.lang.Integer cannot be cast to java.lang.Long
ESM-47102	When you created a resource link by linking the group, if the individual resource was deleted, the Console did not display a prompt asking if you want to delete the resource or remove it from the group. It only asked to confirm the delete. This led to unwanted removal of any other instances of the resource.
ESM-46951	When the property report.csv.header=true was defined in the server.properties file and the report was run in .csv output format, you saw an error similar to the following: [timestamp] com.arcsight.server.reports.ReportException: Failed to archive report [URI], cause by null
ESM-46572	During an actor import using the Model Import Connector, some archive files may be saved with the file name extension .bad. If such files are subsequently manually imported, in some cases it might result in incomplete actor information loaded into the database. This issue does not affect any actors that were successfully imported from the Model Import Connector.
ESM-46301	If you have configured a custom banner, it pops up multiple times while starting the Console.
ESM-41492 TTP#68976	If the severity field was set in a Rules Action Tab and the correlation event was forwarded to an SNMP trap sender or Active Channel, the new severity value didn't get reflected. The severity value was overwritten by the priority value.
ESM-41331 TTP#68451	After the resource validation process is run, assets that are actually invalid appear to be valid. Workaround: Manually mark assets that are known to be invalid as invalid.

Issue	Description
ESM-41272 TTP#68310	Asset Aging tasks will not proceed if you have disabled assets in the system. Workaround: Use one of the following two options: - Fix the invalid assets, or - Ignore the invalid assets by adding the following to the server.properties file: asset.aging.excluded.groups.uris=/All Assets/System Disabled/Disabled Assets
ESM-41168 TTP#68098	Uninstalling and then re-installing the global variable package causes an exception. Global variables are part of the core content and uninstalling core content is not recommended.
ESM-40889 TTP#67567	The "group:101" audit event may fail to be sent in some cases where there are many role memberships being added or changed for an actor. There will be an error in the server log related to this, which includes the IDs of the affected objects.
ESM-40866 TTP#67496	Importing packages or archives containing assets in zones that were modified will cause those assets to become invalid. This happens if you are importing archives from older releases. Workaround: Post import, you need to manually fix the zone for these assets.
ESM-37633 TTP#61154	After installing the Manager, you will see an error in the server.log file: [ERROR][default.com.arcsight.config.util.WebProperties][getPassword] com.arcsight.common.ArcSightException: Cannot handle the data which was obfuscated by old scheme This message is harmless and can be safely ignored.
ESM-37488 TTP#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 file. Additionally, the Manager runs out of memory and therefore automatically restarts itself. Workaround: Use the export format instead of the default format while exporting the rule or Active List definition using an archive or a package. This will not export the Active List data.
ESM-36328 TTP#57661	If the Manager receives a scan for a host that already exists and belongs to a dynamic zone, if the new asset is given a unique domain name, this asset gets created. So, you end up having two assets with the same hostname and dynamic address but different domain names.
ESM-35732 TTP#56123	The Archive tool can occasionally 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: Re-import the same package.
ESM-31433 TTP#46276	You may see the following exception in the Manager's log: 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 Manager's bin directory: arcsight searchindex -a create -m <manager-hostname> -u <admin-user-name> -p <password>

Issue	Description
ESM-30670 TTP#43678	If the search index file becomes corrupted, the Search index will be out-of-date and the following message appears in the Manager's log: [ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF Workaround: Re-generate the index by issuing the following command from the Manager's bin directory: arcsight searchindex -a create
ESM-30314 TTP#42730	You cannot move an asset using Auto Zone if the asset is locked.
ESM-30008 TTP#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.
NGS-1847	InActiveList condition on a multimapped active list does not work when all fields (both key and non-key fields) are not mapped. This does not affect non-multimapped active lists. Workaround: Map all the key and value fields. This is a partial workaround, because all the mapped fields need to match the values stored in the MultiMapAL.
NGS-1718	If an event-based active list contains both a resource reference (for example, Agent Zone) and a related field (for example, Agent Zone Name), then when adding a new active list entry in the Console editor (for example, using the "+" button in the Show Entries display), care should be taken that the related field value matches the value implicit in the resource itself. In the example given, the Zone Name should match the Name of the Zone resource. This can cause some cases of active list lookup (for example, trying to "Edit Entry" in the Show Entries pane), not to match. In this case, it will result in an unpopulated edit pane.
NGS-1449	Some running services depend on other services; for example, the Manager depends on the database. When all ArcSight services are stopped in a single step, either manually or as part of a reboot, the order in which processes actually exit may interfere with such dependencies. When that happens, the service that depends on another may log an error message while shutting down. Such error messages are safe to ignore, because ArcSight services recover from the error condition when they start again.
NGS-264	When integration with iDefense is enabled and you create a Case in ESM, the Case notes may have some special characters garbled. The text can alternately be viewed in iDefense or in the Event Inspector panel.
NGS-172	Base events do not get annotated automatically after rules trigger. Workaround: Annotate the events manually.

ArcSight Web

Issue	Description
ESM-35801 TTP#56258	If you create a Case and set the Estimated Resource Time in ArcSight Web, it does not get set. Workaround: Define this setting on the Console. See the Console online Help for steps to do this.
ESM-35693 TTP#56005	If your session has expired and you click a node in the Navigator tree to expand it, you will see a Java exception and ArcSight Web does not redirect you to the login page.
ESM-33922 TTP#52336	On ArcSight Web, there is no row limit imposed on Query Viewer chart displays (unlike on the ESM Console). Query viewer charts with more than 100 rows do not display properly and are virtually unreadable. On the ESM Console, the chart renders only the first 100 rows and displays an error message indicating that only 100 rows can be properly displayed. No such restriction is available for Query Viewer charts on ArcSight Web dashboards, so rows beyond the 100th row will not display properly on the Web. Workaround: In the Console, set row limits on Query Viewers. This will control chart displays in the Console and ArcSight Web. Determine which Query Viewers you want to display as charts. In the ESM Console, edit those Query Viewers to set the Row Limit to 100 (or less). To do this: 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, if Use Default is enabled, click to deselect it. Then enter a row limit of 100 or less. 3. Click Apply or OK to save the changes.
ESM-30675 TTP#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
NGS-1568	In ArcSight Web, in the Archive Status dashboard->Critical Failure Details, the query viewer shows wrong data for Last Archive Time.

CORR-Engine

Issue	Description
NGS-1821	The import_system_tables command always looks for a database dump file (sql file generated by the export_system_tables command) in the $ARCSIGHT_HOME/tmp/ directory. The import_system_tables command does not accept an absolute path to the dump file, so make sure that the dump file exists in the $ARCSIGHT_HOME/tmp/ directory.
NGS-1696	Long running queries may be terminated by CORR-Engine due to excessive system resource utilization. Sometimes, this could impact event insertion rate or EPS.
NGS-1500	On the first boot up, the CORR-Engine creates and schedules two archives. They are for the same day, and the later one overrides the first one. So, there will be two event archive create and scheduled events in the database.
NGS-1429	You can only restore archives from a single ArcSight Express appliance. Do not combine archives from two different ArcSight Express appliances.

Connectors

Issue	Description
NGS-1423	Upgrading SmartConnector from the ESM Console and Management Console does not work. The SmartConnector does not send upgrade results back to the ESM Console and the Management Console through the Manager.

Installation and Upgrade

Issue	Description
ESM-40984 TTP#67797	Before uninstalling any ArcSight package, certain tasks must be performed in sequence. Remove relationships first before deleting. For example, if the data monitor group is deleted before the data monitor resource, you will encounter a permission error, because permissions are tied to groups.

Management Console

Issue	Description
NGS-1721	If you have the log panel and firebug visible, the event storage configuration scroll bar does not appear completely as a result of which you cannot navigate all the way to the end of the section. Workaround: Either re-size the Firebug panel or refresh the page.
NGS-1670	On Internet Explorer browsers, dashboards that contain tabular view of Data Monitors or Query Viewers sometimes have missing column headers. Reloading the dashboard repeatedly may make the column headers appear.
NGS-1594	Some Dashboards, for example, /All Dashboards/ArcSight Foundation/ArcSight Express/ Cross-Device/Security Activity Statistics, use a fairly large number of Data Monitors and have a lot of information in them that does not translate well to the Image View Dashboards. Such Dashboards are best viewed either using the Console or the ArcSight Web.
NGS-1582	In the Advanced Permissions dialog, if you choose to set permissions on the Field resource, you may see a hidden folder called customCells under your personal folder. This will only happen if you have created some customCells using the ESM Console. If you see such a folder, do not change the ACL settings on it. Doing so will affect the working of custom cells in ESM Console.
NGS-1523	User group creation will fail when the user group name field contains '&'. Workaround: Do not enter '&' in the user group name field.
NGS-1451	If a Dashboard contains a Query Viewer that has a large row limit, the browser may hang while loading this Dashboard. It is a good practice to keep the row limit of Query Viewers below 100 before viewing the Dashboard in custom layout format.
NGS-1435	In the Pie Chart view of a Data Monitor or Query Viewer, if the text in the legend is too long, the pie chart itself will shrink to the extent that it is almost not visible. Workaround: Define a variable to shorten the values that will appear in the legend.

Issue	Description
NGS-1425	The Custom Layout view of a Dashboard, Data Monitor, or Query Viewer displayed in chart view such as bar chart, pie chart or line chart may fail to show due to an issue with the Adobe Flash Player. Workaround: Re-load the Dashboard.
NGS-1283	You must have administrator privileges to access the user/connector management feature.
NGS-1276	The Notification Groups attribute is missing from the user editing page. Workaround: Use the ESM Console to view Notification Groups through Edit User.
NGS-1275	The Notification Groups attribute is missing from connector management page. Workaround:Use the ESM Console to view the Notification Groups through the Configure Connector option.
NGS-1256	After clicking the tab to navigate into a module, you may encounter a blank screen. Workaround: Refresh the screen by reloading the browser page.
NGS-1254	When using some versions of the Firefox browser, occasionally your login fails and you see the following exception in the server.log file: " java.lang.SecurityException: Blocked request without GWT permutation header (XSRF attack?)" This happens because of an issue in Firefox which occasionally drops GWT headers beginning with x. Workaround: Add the following property to the server.properties file: cross.domain.enabled=true and restart the Manager in order for it to take effect.
NGS-1149	If you are using the Internet Explorer browser to access the Management Console, in the "Dashboards" section of the Management Console, the Close Dashboard menu command appears enabled even though it is not an applicable command.
NGS-1072	EventGraph data monitors are not supported on Image Dashboards.
NGS-1071	The Management Console does not support SSL Client Authentication for this release.
NGS-277	You cannot select the docked items (icons such as admin, dashboards etc.) using the keyboard shortcuts. The only way to select them is by using the mouse.

Pattern Discovery

Issue	Description
ESM-46157	In the Profile Actions tab, Global Variables are unavailable for Add to Active List and Add to Session List actions. For example, when Add to Active List is selected for On Pattern Discovered action, the Active List and the Active List field mappings need to be provided. In the drop-down menu of the field mapping, the Global Variables are disabled.
ESM-35048 TTP#54452	A java.lang.InterruptedException might be logged in the ESM Manager server.std.out.logs file when a scheduled Pattern Discovery job is run. The exception is caused by an incorrect database pooling time-out mechanism in the Manager. This does not have any adverse effect on database connections or the functionality of the Pattern Discovery job, and the exception can be safely ignored.
ESM-20555 TTP#24715	In Pattern Discovery, if a profile has event fields with the same name as an event annotation stage name, the snapshot will show a null in the resulting event fields. The snapshot will not be forwarded to the event graph.