Release Notes
ArcSight™ Express

Version 4.5 GA

December 3, 2008

Release Notes ArcSight™ Express,
Version 4.5 GA

Revision History

Date	Product Version	Description
12/03/08	ArcSight™ Express Version 4.5 GA	New Product

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://forum.arcsight.com

Contents

ArcSight Express, Version 4.5 GA

Welcome to ArcSight Express

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Express Storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

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 ArcSight Express successfully, a wizard prompts you to configure ArcSight Express. Refer to the *ArcSight Express Configuration Guide*, which you can download from the ArcSight Customer Support download site.

In this Release

ArcSight Express consists of the ArcSight Express appliance and the ArcSight Express Storage appliance.

The ArcSight Express appliance contains the following components:

- **ArcSight Manager** provides correlation and analytics. It manages, cross-correlates, filters, and processes all security-events in your enterprise. The ArcSight Manager includes a Cross-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.
- **ArcSight Database** stores captured events. It also saves configuration information, such as system users, groups, and permissions and defined rules, zones, assets, and reports.
- **ArcSight Web** is the primary interface for ArcSight Express users, providing access to daily security operations.
- **ArcSight Forwarding Connector** transports events from the ArcSight Express Appliance to the ArcSight Express Storage Appliance.

ArcSight Express does not support Legacy mode in the Forwarding Connector Installation Wizard.

The ArcSight Express Storage appliance contains **ArcSight Logger**, which provides long-term storage for historical search and investigation.

ArcSight Express also comes with a series of coordinated Resources (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. ArcSight Express content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration.

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

Usage Notes

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).

Geographical Information Update

ArcSight Express contains recent geographical information used in graphic displays. The version is GeoIP-532_20080901.

Vulnerability Updates

This release of ArcSight Express includes recent vulnerability mappings (October 2008 Context Update).

Open Issues in ArcSight Express v4.5 GA

These open technical issues merit your review to avoid difficulties.

Refer to the ArcSight Logger v3.0 Release Notes for information about ArcSight Logger open technical issues.

Installation

Number	Description
53324	The First Boot Wizard (FBW) does not validate information in the Logger panel. If you provide the incorrect host name, port number, or receiver information for ArcSight Logger, your appliance will not be set up correctly. **Workaround**: Use care in providing the correct host name, port number, and receiver information in the Logger panel.

Number	Description
53329	The **Java Heap Memory Size** panel in the ArcSight Manager Configuration Wizard displays the default heap size instead of the java heap memory size selected during a previous configuration. **Workaround**: Ensure that you select the appropriate value in the **Java Heap Memory Size** panel whenever you run the ArcSight Manager Configuration Wizard. The recommended heap size for the ArcSight Manager is 2048MB.
53330	The **Java Heap Memory Size** panel in the ArcSight Web Configuration Wizard displays the default heap size instead of the java heap memory size selected during a previous configuration. **Workaround**: Ensure that you select the appropriate value in the **Java Heap Memory Size** panel whenever you run the ArcSight Web Configuration Wizard. The recommended heap size for ArcSight Web is 512MB.
53359	Using an `ssh -X` session to run FBW causes errors and the FBW does not complete. **Workaround**: Instead of using `ssh -X` to run FBW, use `ssh` to connect to the appliance and set your DISPLAY environment variable to point to a valid X11 display.
53977	The FBW does not set up notification and escalation e-mail addresses correctly if multiple comma-separated addresses are specified. **Workaround**: Run the ArcSight Manager Configuration Wizard to specify e-mail notification recipients.

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 assets or cases.
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 you will see the following message 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`

51810 53223	When you start ArcSight Manager, the Manager log records `java.net.SocketException: Socket Closed` errors. These errors are recorded in the logs but do not have a direct impact on the system. You can safely ignore these errors.

Number	Description
53741	If you have imported a large number of scanner reports (for example, more than 10000), the Manager will fail to restart. **Workaround**: In the `server.properties` file, edit the `resource.broker.cache.size.ScannerReport` parameter to specify a value greater than the number of scanner reports you have imported.
53845	ArcSight Manager issues a subsystem warning that the database parameter `undo_retention` is less than the minimum. **Workaround**: To prevent this warning from being issued, add the following line in the `/opt/arcsight/manager/config/server.properties` file and then restart the Manager: `dbcheck.oracle.parameter.undoretention=36000`
53890	When you receive an e-mail notification, you are unable to acknowledge it by replying to the e-mail. **Workaround**: You can acknowledge the e-mail notification from ArcSight Web.
53975	When you set up a pager as the notification destination, no notifications are received on the pager. **Workaround**: If your 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.

ArcSight Console

Number	Description
50968	When 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.
51067	On Windows Vista (64- and 32-bit): ArcSight recommends that you don't install ArcSight Console in the Program Files directory. If you install the Console in the Program Files directory as user *arcsight*, the `console.log` and `velocity.log` files are not created in the logs directory on the Console. **Workaround**: If you want to install ArcSight Console in the Program Files directory on Windows Vista, install it as an admin user.
52098	When you connect to the ArcSight Manager, you encounter an error specifying that the Manager license is not valid. **Workaround**: Import the ArcSight Manager certificate on the ArcSight Console.
53414	On Windows Vista (64-bit), ArcSight Console freezes if a non-admin user tries to export a resource package to certain folders.
53435	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 correct time.

ArcSight Web

Number	Description
24404	In ArcSight Web, channels with conditions that refer to an Event field that ends in `Resource` will fail. ArcSight Web does not support the use of these fields as a filter condition.
43254	Occasionally, when you drill down into the event details in a live channel, the details display for the event, but if you select another event and try to drill down to see its details, you will not be able to do so. **Workaround**: Restart ArcSight Web.
43327	ArcSight Web channels do not support sorting by a time field other than the one chosen as the channel time stamp. For example, a channel in ArcSight Web cannot use Manager Receipt Time as the timestamp and End Time as the sorting timestamp. Attempting to use such a channel in ArcSight Web will produce an error. **Workaround**: Use ArcSight Console to modify the channel sort column and then use it in ArcSight Web.
46969	When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an Active Channel. **Workaround**: Disable error notification in Firefox.
53484	Certain reports run for several hours and then time out or fail with the error message: `com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old` This occurs because Oracle is using a sub-optimal query execution plan. **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*.
53960	If you modify the **Use as Timestamp** field on a channel, you receive an error and the modification is not made.
53961	Filter conditions are lost when you change a channel parameter. This occurs only in ArcSight Web if you provide an invalid parameter value and receive an error. The next time you change the parameter to a valid value and then open the channel, the filter conditions are lost.
53962	Certain channels, such as the built-in live channels, remain at 0% when loading and don't complete even after several minutes. This occurs because Oracle is using a sub-optimal query execution plan. **Workaround**: The issue is corrected when the next statistics update occurs. You can update event statistics manually by running this SQL script: `utilities/database/oracle/common/sql/RegenerateEventStats.sql`

Analytics

50646	The column names of a generated report have a maximum width. If your column name exceeds that limit, the name is truncated and the truncated portion is replaced with a random alphanumeric character. For example, if you create a report that collects two minutes of data for two fields: **Original Agent Translated Zone External ID** and **Original Agent Translated Zone Resource**, the report displays the column names as **Original Agent translated Z** and **Original Agent Translated Z-0**. **Workaround**: Create a short alias for such columns in the report editor.