

Release Notes ArcSight™ Express

Version 4.5 SP1
Build 4.5.1.5926.0

April 20, 2009



Release Notes ArcSight™ Express, Version 4.5 SP1

Copyright © 2009 ArcSight, Inc. All rights reserved.

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

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

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

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
04/20/09	ArcSight™ Express Version 4.5 SP1	Updated Release Notes to include SP1 information

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 SP1	1
Welcome to ArcSight Express	1
Installation and Configuration	1
In this Release	1
Usage Notes	2
Adobe Flash Player Limitation	2
Using ssh Session to Run First Boot Wizard	2
Geographical Information Update	2
Vulnerability Updates	2
Issues Fixed since the v4.5 GA Release	3
Installation	3
ArcSight Manager	3
ArcSight Console	4
ArcSight Web	4
Open Issues in This Release	4
Installation and Upgrade	4
ArcSight Database	5
ArcSight Manager	6
ArcSight Console	6
ArcSight Web	7
Analytics	8
Localization	8

ArcSight Express, Version 4.5 SP1

Welcome to ArcSight Express

ArcSight Express is a Security Information and Event Management (SIEM) system that leverages ArcSight ESM correlation capabilities in combination with an ArcSight Logger storage appliance. Delivers a streamlined, enterprise-level security monitoring and response system through a set of coordinated resources, such as dashboards, rules, and reports, all of which are included as part of the ArcSight Express content.



Refer to the ArcSight ESM v4.5 SP1 Release Notes for information about ArcSight ESM open technical issues.

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

Installation and Configuration

For detailed installation and setup instructions for ArcSight Express, 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 can consist of the ArcSight Express Appliance and the ArcSight Storage Appliance depending on the model purchased.

The ArcSight Express Appliance contains these 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 Storage Appliance.



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

The ArcSight 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

Please review the following points to ensure smooth operation.

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>).

Using ssh Session to Run First Boot Wizard

Using an `ssh -X` session to run First Boot Wizard causes errors and the First Boot Wizard does not complete.

Workaround: Instead of using `ssh -X` to run First Boot Wizard, use `ssh` to connect to the appliance and set your DISPLAY environment variable to point to a valid X11 display.

Geographical Information Update

ArcSight Express contains recent geographical information used in graphic displays. The version is GeoIP-532_20090201.

Vulnerability Updates

This release of ArcSight Express includes recent vulnerability mappings (February 2009 Context Update).

Device	Vulnerability Updates
McAfee HIPS 7.0	Updated CVE, MSSB
Radware DefensePro	Updated CVE, MSSB

Device	Vulnerability Updates
Cisco Secure IDS S376	Updated Bugtraq, CVE
FunkWerk (VarySys Technologies) PacketAlarm	Updated Bugtraq, CVE, Nessus, Arachnids, MSSB
Juniper/Netscreen IDP update 1349	Updated Bugtraq, CVE, MSSB, X-Force, CERT, MSKB
McAfee Intrushield	Updated CVE, MSSB
TippingPoint UnityOne DV7626	Updated CVE, Bugtraq, MSSB
Snort / Sourcefire SEU 189	Updated Bugtraq, MSSB, CVE
Fortigate Fortinet	Bugtraq, CVE, MSSB, X-Force
ISS SiteProtector	Updated X-Force, CVE, CERT, Bugtraq, MSSB

Issues Fixed since the v4.5 GA Release

Installation

Number	Description
53324	The First Boot Wizard did not validate information in the Logger panel. If you provided the incorrect host name, port number, or receiver information for ArcSight Logger, your appliance would not be set up correctly.
53329	The Java Heap Memory Size panel in the ArcSight Manager Configuration Wizard displayed the default heap size instead of the java heap memory size selected during a previous configuration.
53330	The Java Heap Memory Size panel in the ArcSight Web Configuration Wizard displayed the default heap size instead of the java heap memory size selected during a previous configuration. The Java Heap Memory Size now gets transferred during upgrade.

ArcSight Manager

Number	Description
51810 53223	When you started ArcSight Manager, the Manager log records <code>java.net.SocketException: Socket Closed</code> errors. These errors were recorded in the logs but did not have a direct impact on the system.
53741	If you imported a large number of scanner reports (for example, more than 10000), the Manager would fail to restart.
53845	ArcSight Manager issued a subsystem warning that the database parameter <code>undo_retention</code> was less than the minimum.

ArcSight Console

Number	Description
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 <i>arcsight</i> , the <i>console.log</i> and <i>velocity.log</i> files are not created in the logs directory on the Console.
52098	When you connected to the ArcSight Manager, you encountered an error specifying that the Manager license was not valid. This has now been fixed such that the Manager license gets validated after you accept the Manager's certificate when prompted.
53414	On Windows Vista (64-bit), ArcSight Console froze if a non-admin user tried to export a resource package to certain folders.

ArcSight Web

Number	Description
53960	If you modified the Use as Timestamp field on a channel, you received an error and the modification was not made.
53961	Filter conditions were lost when you changed a channel parameter. This occurred only in ArcSight Web if you provided an invalid parameter value and received an error. The next time you changed the parameter to a valid value and then opened the channel, the filter conditions were lost.

Open Issues in This Release

These open technical issues merit your review to avoid difficulties.

Installation and Upgrade

Number	Description
53359	Using an <i>ssh -X</i> session to either upgrade ArcSight Express or run FBW causes errors and the FBW does not complete. Workaround: Instead of using <i>ssh -X</i> to run FBW or upgrade ArcSight Express, use <i>ssh</i> to connect to the appliance and set your <i>DISPLAY</i> environment variable to point to a valid X11 display.
55289	If you start the wizard to configure ArcSight Database using the <i>./arcsight database pc</i> command, please modify the Manager host name and Database user name and their passwords to match the host names and passwords that you had set up in the First Boot Wizard panel. These values do not get updated with the setting you had provided when running the First Boot Wizard.

Number	Description
55381	<p>When upgrading the software on ArcSight Express, you will see the following error message in the Forwarding Connector log:</p> <pre>INFO jvm 1 2009/02/09 17:03:47 com.arcsight.common.ArcSightException: ISSFAILURE:[Database Connection: Received exception while trying to check connectivity to the database: Io exception: Got minus one from a read call</pre> <p>This message is harmless and can be safely ignored.</p>
55476	<p>If you open 10 channels and view them then delete these 10 channels from the resource tree, you will not be able to open any more channels. You will see the following error:</p> <pre>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.</pre> <p>Workaround: Restart the Console.</p>
55964	<p>When running the First Boot Wizard, be sure you do not change the default values in the Hosts tab of the Network Settings panel. If you change the default values, it could lead to loss of network connectivity and you will receive this error:</p> <pre>Could not look up internet addresses for <hostname>.This will prevent GNOME from operating correctly.</pre>
56179	<p>Any errors while configuring the host name or IP address of the machine in the First Boot Wizard will cause the <code>localhost</code> entry to be removed from the <code>/etc/hosts</code> file. Consequently, the First Boot Wizard will fail.</p> <p>Workaround: If you want to change the host name or IP address after you have configured them using the First Boot Wizard, you have to do a system restore and make the changes in the First Boot Wizard itself.</p>
55746	<p>If Oracle, TNS Listener, Web and Manager are down before doing an upgrade, you will see FATAL EXCEPTION errors in your <code>aeupdate</code> log, even though the upgrade will proceed smoothly and succeed.</p> <p>These errors are safe to ignore.</p>

ArcSight Database

Number	Description
53484	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <pre>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</pre> <p>This occurs because Oracle is using a sub-optimal query execution plan. In some cases, this can happen because of insufficient space in the ARC_TEMP table as well.</p> <p>Workaround: Set the report to query with a full scan database hint. For more information, refer to "Reports that query over a large time range with complex joins take a long time to run" in Appendix B of the <i>ArcSight ESM Administrator's Guide</i>.</p>

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	<p>If the search index file becomes corrupted, the Search index will be out-of-date and you will see this message in the Manager log:</p> <pre>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init] java.io.IOException: read past EOF</pre> <p>Workaround: Regenerate the index by issuing this command from the Manager <ARCSIGHT_HOME>/bin directory:</p> <pre>arcsight searchindex -a create</pre>
53975	<p>If you are not able to setup sending pager notifications through the pager service provider, please follow the workaround provided.</p> <p>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.</p>

ArcSight Console

Number	Description
50968	<p>When you delete an escalation-level notification resource, you receive the error <code>Group does not exist</code> in the <code>console.log</code> file.</p> <p>This error is incorrect and can be ignored.</p>
53435	<p>When you set the Schedule Frequency for a report, the Next Run Time field displays incorrectly in the Editor.</p> <p>Even though the time displays incorrectly, the report runs at the correct time.</p>
55810	<p>When upgrading the ArcSight Console, you will be prompted to enter the path to the previous Console installation. Be sure to provide the path to the <code>current</code> directory of your previous Console installation. If you do not point to the <code>current</code> directory, you will get an error that the <code>cacerts</code> folder could not be found in this location. Selecting OK will allow you to continue with the upgrade. But, this will cause the certificates to not get transferred and make the upgrade error prone.</p>
53822	<p>If you try to open an archived report in the Console, it fails to open. This happens only the first time when you try this after an upgrade or a fresh installation.</p> <p>Workaround: Restart the Console.</p>

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	<p>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.</p> <p>Workaround: Restart ArcSight Web.</p>
43327	<p>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.</p> <p>Workaround: Use ArcSight Console to modify the channel sort column and then use it in ArcSight Web.</p>
46969	<p>When you use ArcSight Web with the Firefox web browser, you might encounter an error if you refresh an Active Channel.</p> <p>Workaround: Disable error notification in Firefox.</p>
55995	<p>On ArcSight Web "Active Channels", the Event Inspector "Create Channel" feature does not create the channel filter properly.</p> <p>Clicking an event in an active channel brings up the Event Inspector, where you can view details on event fields or create a channel based on the value in an event field. Options are provided to (1) create a channel that filters only on the selected event field value or (2) add the selected event field value as a condition to the current channel filter. Option (1) does not work correctly, but instead simply adds the selected field value to the filter the same way option 2 does.</p> <p>Workaround: Manually modify the filter to specify the conditions you want. For example, to create a channel on an event field value for Priority, click an event in a channel to get the Event Inspector, click the Priority field and choose Create Channel [Priority=<value>] or Create Channel [Priority != <value>]. At this point, the filter conditions will not display correctly. Click "Modify", and edit the Condition Summary to remove the extra conditions and include only the values you want to filter for, e.g.: Priority = "3". Now click "'Open" to view the modified channel or "Save Filter As..." to save it.</p>
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.
56821	Mozilla Firefox 1.5 browser is not supported on ArcSight Express. Please do not use this browser to access ArcSight Web.

Analytics

50646	<p>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.</p> <p>Workaround: Create a short alias for such columns in the report editor.</p>
54713	<p>If you had scheduled a report to run every two hours before the start of Daylight Saving Time (DST) 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 will occur on odd numbered hours (for example 1:00 am, 3:00 am, etc.). The interval will continue to be every 2 hours.</p>
54749 55835	<p>Depending on your time zone, you may see your scheduled tasks running off by 15 minutes to an hour. For example, scheduled tasks will run 15 minutes early in America/Guyana, whereas in Asia/Bahrain or Europe/London it will run one hour early, etc.</p>
55230	<p>When viewing reports you might encounter timestamps that are off by an hour.</p> <p>To convert the time in the database to your local time, the current time zone setting (including any DST offset) will be used. If the times you are querying are in a different DST setting, the local time reported will be off by one hour. For example, if you are in the Pacific timezone and in DST, and the time range you are querying is not in DST, the time will be off by one hour. For example, if it is June (in DST) and you query times in January (not in DST), your times will be corrected by the current timezone setting (in DST), even though the January times should not have DST applied to them</p>
56258	<p>When you create a Case, if you set the Estimated Restore Time, it does not get set.</p>
56345	<p>If your query uses the getSessionData variable to join a session list with an active list you will get an error when you try to run the report or view the channel.</p>

Localization

55823	<p>In Traditional Chinese and Japanese environments: After assigning a hotkey to a resource the Console does not restart.</p> <p>Workaround: Edit the keymap.xml file in the Console's <code><ARCSIGHT_HOME>/config/console</code> directory and remove the <code><action></code> tag which contains the non-English characters. Be sure to delete all the lines starting with <code><action></code> tag and ending with <code></action></code> including the tag line itself.</p>
-------	--