

Release Notes ArcSight™ Express

Version 4.5 SP2
Build 4.5.2.6076.0

January 18, 2010



Release Notes ArcSight™ Express, Version 4.5 SP2

Copyright © 2010 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
01/18/10	ArcSight™ Express Version 4.5 SP2	Updated Release Notes to include SP2 information
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 SP2	1
Welcome to ArcSight Express	1
Purpose of this Release	1
Localization	1
Japanese and Traditional Chinese	2
French	2
Installation and Configuration	2
In this Release	2
Usage Notes	3
Adobe Flash Player Limitation	3
Using ssh Session to Upgrade or Run First Boot Wizard	3
Geographical Information Update	4
Vulnerability Updates	4
Issues Fixed in this Patch	4
Installation and Upgrade	4
Open Issues in This Release	5
Installation and Upgrade	5
ArcSight Database	6
ArcSight Manager	7
ArcSight Console	7
ArcSight Web	8
Analytics	9
Localization	9

ArcSight Express, Version 4.5 SP2

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.



Note

Refer to the *ArcSight ESM v4.5 SP2 Release Notes* for information about ArcSight ESM open technical issues.

Refer to the *ArcSight Logger v4.0 Release Notes* for information about ArcSight Storage Appliance open technical issues.



Caution

If you are upgrading from an older version of ESM, you are required to upgrade to all the interim versions one at a time, before upgrading to v4.5 SP2.

For example, if you are upgrading from v4.5 GA to v4.5 SP2, you will be required to first upgrade your v4.5 GA installation to v4.5 SP1 before upgrading to v4.5 SP2. See the *Upgrading ArcSight Express from v4.5 GA to v4.5 SP1* document for details on upgrading to v4.5 SP1.

Purpose of this Release

The purpose of this Service Pack is to:

- update translation packages for Japanese, Traditional Chinese, and French
- address customer requested and other issues
- Updates for geographical information and vulnerability mapping
- provide Oracle CPU certification with currently available CPU of October 2009 Update

Localization

To configure the First Boot Wizard for localization of Japanese, Traditional Chinese, and French, complete the following steps.



Note

The following steps are only necessary for users on

M7100 appliance and

M7200 appliance, 4.SP1 Patch 2

Japanese and Traditional Chinese

After you have completed configuration of the OS, "Finish Setup" appears on the screen.

- 1 Click **Next**.
- 2 When prompted on the "Enterprise Linux" screen, log in as user "root".
- 3 Retain this screen.
- 4 From directory `/opt/arcsight/manager/il8n/common/`, modify the following property files:

Japanese: `common_strings_jp.properties`

Traditional Chinese: `common_strings_zh_TW.properties`
- 5 Comment out any of the following property: `schedule.frequency.*`
- 6 Continue within the "ArcSight Express Configuration Wizard" to complete the remaining steps of configuration.

French

After you have completed configuration of the OS, "Finish Setup" appears on the screen.

- 1 Click **Next**.
- 2 When prompted on the "Enterprise Linux" screen, log in as user "root".
- 3 From the "Welcome to ArcSight Express" screen, cancel the First Boot Wizard.
- 4 Open a shell and export the following environment variable:

`ARCSIGHT_LOCALE=ALL`

`export ARCSIGHT_LOCALE`
- 5 Restart the wizard by typing:

`cd /opt/arcsight/manager/bin`

`arcsight appliancefirstbootsetup`
- 6 Under the **Select Language/Local** drop-down menu, choose **fr_FR.UTF-8**.
- 7 Continue within the "ArcSight Express Configuration Wizard" to complete the remaining steps of configuration.

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 Upgrade or Run First Boot Wizard

Using an `ssh -X` session to either upgrade ArcSight Express or run FBW causes errors and the FBW does not complete.

Workaround: Instead of using `ssh -X` to run FBW or upgrade ArcSight Express, 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_20091201.

Vulnerability Updates

This release includes recent vulnerability mappings (December 2009 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 281	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Enterasys Dragon IDS	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Cisco Secure IDS S457	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
McAfee Intrushield	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
TippingPoint UnityOne DV7859	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Fortinet Fortigate	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
ISS SiteProtector	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Symantec Endpoint Protection	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
McAfee HIPS 7.0	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Radware DefensePro	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
FunkWerk (VarySys Technologies) PacketAlarm	Arachnids, Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB

Issues Fixed in this Patch

Installation and Upgrade

Number	Description
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>

Open Issues in This Release

These open technical issues merit your review to avoid difficulties.

Installation and Upgrade

Number	Description
53359	<p>Using an <code>ssh -X</code> session to either upgrade ArcSight Express or run FBW causes errors and the FBW does not complete.</p> <p>Workaround: Instead of using <code>ssh -X</code> to run FBW or upgrade ArcSight Express, use <code>ssh</code> to connect to the appliance and set your <code>DISPLAY</code> environment variable to point to a valid X11 display.</p>
53977	<p>SBR: didn't received warning email when free tablespace is under 5%.</p>
55289	<p>If you start the wizard to configure ArcSight Database using the <code>./arcsight database pc</code> 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.</p>
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>

Number	Description
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>
60111	<p>For M7200 series only: While running the First Boot Wizard, you may encounter an error:</p> <p><code>"Fatal errors encountered. Could not proceed."</code></p> <p>This indicates that there was an error when setting up one of the Network Configuration panels.</p> <p>Workaround: Check the <code>/opt/arc sight/manager/logs/firstboot.log</code> file to see where the error occurred. Also, refer to "Appendix A, Troubleshooting" in the <i>ArcSight Express Configuration Guide</i> for more details on this error and how to resolve it.</p>
60455	<p>For M7200 series only: After completing the First Boot Wizard successfully, if you reboot the ArcSight Express Appliance, you will see a panel from the First Boot Wizard which tells you that all components have been successfully configured.</p> <p>Workaround: Exit the wizard panel by clicking the Cancel button.</p>
60767	<p>If you are using the X Windows functionality to remotely access ArcSight Express to apply the patch, you might run into this error:</p> <p><code>X11 connection rejected because of wrong authentication.</code></p> <p>This error is an indication that your content packages have not been updated.</p> <p>Workaround: Run the following from a shell prompt:</p> <pre>arc sight patchcontentinst</pre> <p>to update the content packages.</p>
61714	<p>When upgrading from ESM 4.5 SP1 Patch 2/Patch 3, to ESM 4.5 SP2, the dbcheck script will give you an error.</p> <p>Workaround: Do the following before running the <code>arc sight dbcheck</code> command:</p> <ol style="list-style-type: none"> 1 Open a shell window and go to the Database's <code><ARCSIGHT_HOME>/bin/scripts</code> directory. 2 Run the <code>dos2unix dbcheck.sh</code> command.

ArcSight Database

Number	Description
53484	<p>Certain reports run for several hours and then time out or fail with the error message:</p> <p><code>com.arcsight.common.persist.PersistenceException: Unable to execute query: ORA-01555: snapshot too old</code></p> <p>This occurs because Oracle is using a sub-optimal query execution plan. In some cases, this can happen because of insufficient space in the ARC_TEMP table 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>

Number	Description
53977	<p>When available database free space in tablespace reduces to 5% or less, a warning email should be sent to the notification email address list. Frequently, this message is not activated. This can be monitored from the console using the dashboards.</p> <p>Workaround: Monitor the Arc_Event_Data table to verify that the "% Free" column is over 5% at all times.</p>
62989	<p>SBR for M7100/M7200: When the following error occurs:</p> <p>error Cause: <code>ORA-01013: user requested cancel of current operation</code></p> <p>set the value of the parameter <code>partition.manager.updatestats.query.timeout</code> to a larger value (e.g., 14400).</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> <p><code>[ERROR][default.com.arcsight.server.search.index.IndexResources][_init]</code></p> <p><code>java.io.IOException: read past EOF</code></p> <p>Workaround: Regenerate the index by issuing this command from the Manager <code><ARCSIGHT_HOME>/bin</code> directory:</p> <p><code>arcsight searchindex -a create</code></p>
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>

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 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.
53822	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. Workaround: Restart the Console.

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.
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>
-------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

