

ArcSight Express All-in-One™ Release Notes

Version 2.0

includes
ArcSight Express™ v5.0 SP1 Patch 2
ArcSight Logger™ v5.1

November 8, 2011



ArcSight Express All-in-One™ Release Notes Version 2.0

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

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

This document is confidential.

Revision History

Date	Product Version	Description
11/8/2011	ArcSight Express All-in-One™ version 2.0 (with ArcSight Express™ v5.0 SP1 Patch 2 and ArcSight Logger™ v5.1)	Added reminder to download the license key before upgrading
8/25/2011	ArcSight Express All-in-One™ version 2.0 (with ArcSight Express™ v5.0 SP1 Patch 2 and ArcSight Logger™ v5.1)	Release Notes for ArcSight Express All-in-One™ v2.0

ArcSight Customer Support

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

Contents

ArcSight Express All-in-One™
Version 2.0 5

 Welcome to ArcSight Express All-in-One™ 5

 Release Contents 6

 Section 508 Compliance 6

 Usage Notes 6

 Upgrading ArcSight Express All-in-One 6

 Issues Fixed in this Release 6

 Open Issues in this Release 7

ArcSight Express All-in-One™

Version 2.0

Welcome to ArcSight Express All-in-One™

ArcSight Express All-in-One is a Security Information and Event Management (SIEM) system that leverages ArcSight Express™ correlation capabilities in combination with ArcSight Logger™ in a single appliance. ArcSight Express All-in-One 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.

Topics in the Release Notes:

["Release Contents" on page 6](#)

["Section 508 Compliance" on page 6](#)

["Usage Notes" on page 6](#)

["Issues Fixed in this Release" on page 6](#)

["Open Issues in this Release" on page 7](#)



If you have the V7200 appliance, download the updated license file from <https://arcsight.subscribe.net.com> before upgrading the appliance.

Release Contents

ArcSight Express All-in-One™ includes the following software components:

- ArcSight Express™ version 5.0.1.6642.2
- ArcSight Forwarding Connector version 5.0.2.5672.0
- ArcSight Logger™ version 5.1.5887
 - ◆ ConnApp connector container 1 version 5.1.2.5823.0
 - ◆ ConnApp connector container 2 version 5.1.2.5823.0
 - ◆ ArcSight TRM™ version 5.0
- ArcSight IdentityView™ Express version 1.1 SP1
- ArcSight Microsoft Active Directory Model Import SmartConnector for ArcSight ESM version 4.7.6.5515.0



For details about each software component, refer to the respective release notes.

Section 508 Compliance

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

Usage Notes

Upgrading ArcSight Express All-in-One

An upgrade is available for ArcSight Express All-in-One. This upgrade applies to model V7400 after initial configuration and initialization is completed. This upgrade also applies to existing ArcSight Express All-in-One deployments as in the model V7200. Refer to the document, *ArcSight Express Upgrade Guide*, *ArcSight Express All-in-One 2.0* for details.

After installing the updates and rebooting the appliance, ArcSight Manager may not automatically start. Rebooting again should fix this problem. You can also start Manager manually. Refer to the *Configuration Guide* for ArcSight Express All-in-One, *Troubleshooting* chapter, for a list of commands to start and stop services.

Issues Fixed in this Release

The following issue has been resolved in this release.

Issue	Description
CONAPP-2247	<p>Retrieving backup container files from the repository displayed an error.</p> <p>On the Logger UI, if you select Configuration > Repositories > Backup Files, then click Retrieve Container Files and select the container you want to retrieve, the following message is displayed:</p> <p>Error (Null)</p> <p>This is because the backup files could not be found. This is now fixed.</p>

Open Issues in this Release

This release contains the following open issues with the recommended workarounds.

Issue	Description
ESM-45558	<p>If you have added the ArcSight TRM SmartConnector and you are upgrading or performing an emergency restore on the SmartConnector in Container 1, the SmartConnector may not function properly after the upgrade or restore process.</p> <p>Workaround:</p> <p>As root, enter the following commands:</p> <pre>cd /opt/arcsight mkdir -p connector_1/current/jre/lib/endorsed/ cp -pv trm/local/tomcat/webapps/nwsapi/WEB-INF/lib/saaj.jar \ connector_1/current/jre/lib/endorsed/ /sbin/service arc_appliance_connector_1 restart</pre>
ESM-47903	<p>IdentityView 2.0 SP1 is supported but not included in the ArcSight Express All-in-One distribution. If you are interested in IdentityView, download the IdentityView file, including the Active Directory Model Import Connector, from the ArcSight Download Center at https://arcsight.subscribenet.com.</p>
ESM-47993	<p>After Logger is restored from backup, the original settings from the database are restored for network interfaces, hosts, IP/gateway, and so on. These are different from what the user has set up for the ArcSight Express All-in-One appliance using the OS First Boot Wizard. The appliance therefore is not able to connect to the network.</p> <p>Workaround:</p> <p>After restoring Logger from backup, re-enter the appliance's network settings in Logger's System Admin page for DNS Settings, Hosts, and Network tabs to ensure consistency with what was entered during First Boot Wizard configuration.</p>
ESM-48176	<p>After upgrading the ArcSight Express All-in-One appliance, the TRM Service may not start up after it is added.</p> <p>Workaround:</p> <ol style="list-style-type: none"> Run the following command: <pre>chmod -R 700 /opt/arcsight/trm/local/pgsql/data</pre> Start the TRM service.

Issue	Description
NSP-3902	<p>The Support Logs option for Threat Response Manager does not generate expected logs. On the NSP UI for Threat Response Manager (TRM), if you select Admin > Error Log and click Support Logs, no logs are displayed. Logs are in the following locations:</p> <pre> /opt/arcsight/trm/local/apache/logs/access_log* /opt/arcsight/trm/local/apache/logs/error_log* /opt/arcsight/trm/local/pgsql/data/serverlog* /opt/arcsight/trm/local/tomcat/logs/* /var/log/messages /var/log/secure /var/log/dmesg /opt/updates/*.log /opt/arcsight/trm/ENIRA/data/temp/* /opt/arcsight/trm/ENIRA/data/debug/* /opt/arcsight/trm/ENIRA/data/insp_log* /opt/arcsight/trm/ENIRA/data/exceptions.log* </pre> <p>Workaround:</p> <ol style="list-style-type: none"> 1. As root, run the following script as a one-time process on the ArcSight Express All-in-One appliance: <pre> cd /opt/arcsight/trm/ENIRA sed -i -re '/SystemStats->new/,/close.STATFILE/s/^/#/' \ OS/SystemInfo.pm sed -i -re 's#`(/opt.*openssl enc)#`/bin/env OPENSSL_FIPS=0 \1#' \ Crypt/Engine.pm </pre> 2. Access the NSP UI for Threat Response Manager (TRM) and follow instructions in the Online Help on how to download Support Logs. 3. Send the downloaded logs to ArcSight Customer Support.
NSP-3904	<p>A certificate for Threat Response Manager is not generated and prevents the user from installing the required signed CA certificate.</p> <p>On the NSP UI for Threat Response Manager (TRM), if you select Admin > System > SSL Certificate > Generate CSR, the private key server.pem is not created. This key is expected to be created in opt/local/openssl/private.</p> <p>Workaround:</p> <p>As root, run the following commands:</p> <pre> file=/opt/arcsight/trm/ENIRA/OS/SSL.pm commandRE='(/opt/local/openssl/bin/openssl\s+(genrsa rsa req x509))' sed -i -re "s#\\$commandRE#env OPENSSL_FIPS=1 \0#" \$file service trm restart httpd </pre> <p>Follow the instructions in the ArcSight NSP Installation and Administrator's Guide on how to use the NSP UI to generate and download the CSR.</p>