ArcSight Express All-in-One Release Notes

Version 4.5 SP2, Patch 2

April 22, 2011

ArcSight™
An HP Company

ArcSight Express All-in-One Release Notes
Version 4.5 SP2, Patch 2

Copyright © 2011 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
4/22/2011	ArcSight Express All-in-One version 4.5 SP2 Patch 2	Added the section, "Corrections to the Configuration Guide" on page 6
9/3/2010	ArcSight Express All-in-One version 4.5 SP2 Patch 2	Initial release of this Release Notes

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 4.5 SP2, Patch 2

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 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

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

- ArcSight ESM version 4.5 SP2 Patch 2
- ArcSight Forwarding Connector version 4.7.6.5416.0
- ArcSight Logger version 4.5 GA
  - ConnApp connector container 1 version 4.7.7.5427.0
  - ConnApp connector container 2 version 4.7.7.5427.0
- 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

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.

Corrections to the Configuration Guide

This section describes errors found in the ArcSight Express All-in-One Configuration Guide v4.5 SP2 and provides the corrections. Page numbers are based on the guide's physical page and not the PDF page.

Location in the Guide	Description of Error and Correction
Chapter 2, Configuring ArcSight Express All-in-One	
Define Storage Volume, p. 30	For defining storage volume for the storage appliance, the guide specifies: Set the maximum size to 1024 GB. **Correction:** Instead of *1024 GB*, the maximum size should be **900 GB**.
Create Storage Groups, p. 30	The first sentence under this topic states: After you create the Storage Volume, define the Default Storage Group. **Correction:** Instead of *create*, the sentence should state **configure**: After you create the Storage Volume, **configure** the Default Storage Group. This is because Default Storage Group is already defined in the system. You only need to configure the values.
	In the example for creating another storage group, the guide states: For example, if your maximum size is 700 GB for the first storage group, the remaining availabe space for the next group will be 324 GB. **Correction:** Instead of *324 GB*, the value should be **195 GB**.

Location in the Guide	Description of Error and Correction
Appendix B, Default Settings for Components	
ArcSight Database, p. 74	Sizing information is provided as follows: ARC_EVENT_DATA = 400 GB (25 files * 16 GB) ARC_EVENT_INDEX = 800 GB (50 files * 16 GB) ARC_UNDO = 96 GB (12 files * 8GB) ARC_TEMP = 48 GB (6 files * 8GB) **Corrections:** The sizing information should be ARC_EVENT_DATA = **96 GB (6 files x 16 GB)** ARC_EVENT_INDEX = **192 GB (12 files x 16 GB)** ARC_UNDO = **64 GB (8 files x 8 GB)** ARC_TEMP = **32 GB (4 files x 8 GB)** Generally, the sizes should be smaller than what was originally documented.

Open Issues

This release contains the following open issues. Use the workarounds noted.

Number	Description
CONAPP-2247	**Retrieving backup container files from the repository displays an error.** 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: `Error (Null)` This is because the backup files cannot be found. **Workaround**: The backup files are found in `/opt/arcsight/connector_X/current/user/agent`, where ***X*** is the container number. You may copy the desired file from that directory.

ESM-45558	**Upgrading the ArcSight Threat Response Manager (TRM) SmartConnector**
	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.
	Workaround:
	As **root**, enter the following commands:
	`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`

Number	Description

NSP-3902	**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:
	• /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*
	Workaround:
	1 As **root**, run the following script as a one-time process on the ArcSight Express All-in-One appliance:
	`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`
	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	**A certificate for Threat Response Manager is not generated and prevents the user from installing the required signed CA certificate.**
	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`. The result is that you will not be able to upload a signed certificate through the UI.
	Workaround:
	1 As **root**, run the following commands:
	`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`
	2 Follow the instructions in the *ArcSight NSP Installation and Administration Guide* on how to generate and download the Certificate Signing Request (CSR).