

Release Notes ArcSight™ Express

Version 5.0 SP1 Patch 1

March 24, 2011



Release Notes ArcSight™ Express, Version 5.0 SP1 Patch 1

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
3/24/11	ArcSight™ Express Version 5.0 SP1 Patch 1	Released with ESM v5.0 SP1 Patch 1

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, Version 5.0 SP1 Patch 1 5
 - Welcome to ArcSight Express 5
 - Purpose of this Release 5
 - Pattern Discovery Enhancement 5
 - Section 508 Enhancements 5
 - Console Platform Support 6
 - Geographical Information Update 6
 - Vulnerability Updates 6
 - JRE Update 6
 - Issues Fixed in this Release 7
 - ArcSight Console 7
 - Installation 7
 - Open Issues in this Release 7
 - Connectors 8
 - General 8
 - Installation and Upgrade 9

ArcSight Express, Version 5.0 SP1 Patch 1

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. 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.

The following topics are covered:

- [“Purpose of this Release” on page 5](#)
- [“Console Platform Support” on page 6](#)
- [“Geographical Information Update” on page 6](#)
- [“Vulnerability Updates” on page 6](#)
- [“JRE Update” on page 6](#)
- [“Issues Fixed in this Release” on page 7](#)
- [“Open Issues in this Release” on page 7](#)

Purpose of this Release

Below is a high level summary of the improvements introduced with ESM v5.0 SP1. For a more detailed information, refer to the following sources of information:

- The *What's New* topic in the product's online documentation
- The Release Notes for ArcSight ESM 5.0 Service Pack 1

Pattern Discovery Enhancement

As part of ESM v5.0 SP1, Pattern Discovery introduces support for local and global variables as well as domain fields.

Section 508 Enhancements

ArcSight Web now provides a warning when an active session is about to time out and provides the option to continue the session.

Console Platform Support

Platform	Supported Operating System	Typical System Requirements
Linux	Red Hat Enterprise Linux (RHEL 5.4 and 5.5) Desktop 32-bit	x86-compatible multi-CPU system with 2-4 GB RAM
Macintosh OS X	Macintosh OS X 10.6 64-bit	
Windows	Microsoft Windows 7 64-bit Microsoft Windows Vista SP2 64-bit Microsoft Windows XP Professional SP3 32-bit	x86-compatible single or multi-CPU system with 1-2 GB RAM

Geographical Information Update

The version of ESM in this release includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20101101.

Vulnerability Updates

This release includes recent vulnerability mappings (November 2010 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 388	Faultline, Bugtraq, CVE, Nessus, MSSB
Enterasys Dragon IDS	Faultline, CVE, MSSB
Cisco Secure IDS S529	Faultline, Bugtraq, CVE, Nessus
McAfee Intrushield	Faultline, CVE
TippingPoint UnityOne DV8131	Faultline, Bugtraq, CVE, MSSB
Fortinet Fortigate	Bugtraq, MSSB
ISS SiteProtector	CVE
Symantec Endpoint Protection	Faultline, Bugtraq, CVE
McAfee HIPS 7.0	Faultline, CVE
Radware DefensePro	CVE

JRE Update

Important!

You must apply a hotfix to update the Java Runtime Environment (JRE) on the appliance. The hotfix addresses the Security Alert for CVE-2010-4476.

Refer to the document, [AE_AIO_Hotfix-CVE-2010-4476_ReadMe.txt](#), for specific steps on how to apply the hotfix on the ArcSight Express appliance. Contact Customer Support if you require assistance.

Issues Fixed in this Release

The following links will take you to issues you might encounter as you go through the workflow of installing, configuring, and using the product features:

- [Installation](#)
- [ArcSight Console](#)

ArcSight Console

Issue	Description
ESM-45937	After applying v5.0 Patch 1, when you connect to ESM using the Console and launch either a custom view dashboard or an external browser, the system displays a blank screen. This happens only on first connection after an upgrade or after a fresh installation, at the point where you import the Manager certificate using the Console wizard screen that prompts you to select your authentication type.
ESM-34779 TTP#53822	If you try to open an archived report in the Console, the report fails to open. This happens only the first time when you try this after an upgrade or a fresh installation, where you import the Manager certificate using the Console wizard screen that prompts you to select your authentication type. Workaround: Restart the Console.

Installation

Issue	Description
ESM-45622	A fresh install of ArcSight Express displays an SSL Handshake error on the Console.

Open Issues in this Release

The following links will take you to issues you might encounter as you go through the workflow of installing, configuring, and using the product features:

- [Installation and Upgrade](#)
- [Connectors](#)
- [General](#)

Connectors

Issue	Description
ESM-45903	A Java IOException (Cannot run program "/usr/bin/tw_cli /c0 show all") will be thrown on the ArcSight Express models M7100 and M7200 after upgrading from 4.5 build to 5.0 Patch 1. This exception will not affect the performance of the onboard Forwarding connector.

General

Issue	Description
ESM-47279	<p>If you enabled the firewall on the Network Setup dialog, kept the default trusted services (ArcSight Manager and ArcSight Web) selected, and modified firewall settings further by adding a port as an example, connection to ESM Manager will not be possible. This is because a new firewall file is written as a result of the modification. The IPtables will not be able to resolve the ports with the new firewall file.</p> <p>Workaround:</p> <ul style="list-style-type: none"> - Either add the "a_mgr" and "a_web" to /etc/services, for example: <pre>echo -e "a_mgr 8443/tcp\na_web 9443/tcp" >> /etc/services</pre> Or - When specifying the firewall settings manually, include 8443:tcp, 9443:tcp as appropriate (rather than use the ArcSight Web or ArcSight Manager checkboxes).
ESM-45272 TTP#53359	<p>Using an ssh -X session to either upgrade ArcSight Express or run FBW causes errors and the FBW does not complete.</p> <p>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.</p>
ESM-38831 TTP#63302	<p>When specifying a password for the database user account "arcsight," even if you follow the rules for Oracle passwords (begin with a letter followed by any combination of letters, numbers, and the special characters \$ # _), if your password contains the \$ sign, the First Boot Wizard will fail with a fatal error during the Manager setup stage.</p> <p>Workaround: Do not use the \$ sign while specifying the password for the database user account, "arcsight."</p>
ESM-35370 TTP#55289	<p>If you start the wizard to configure ArcSight Database using the ./arcsight database pc command, 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>

Installation and Upgrade

Issue	Description
ESM-35418 TTP#55381	<p>When upgrading the software on ArcSight Express, you will see the following error message in the Forwarding Connector log:</p> <p>INFO jvm 1 2009/02/09 17:03:47 com.arcsight.common.ArcSightException:</p> <p>ISSFAILURE:[Database Connection: Received exception while trying to check connectivity to the database: Io exception: Got minus one from a read call</p> <p>This message is harmless and can be safely ignored.</p>

