

Release Notes ArcSight™ Express

Version 5.0 Patch 1
Build 5.0.0.6521.1

April 22, 2011



Release Notes ArcSight™ Express, Version 5.0 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
4/22/2011	ArcSight™ Express Version 5.0 Patch 1	Added item to " Upgrade-related Notes " on page 7 on performing updates to ArcSight Express All-in-One appliance
11/4/2010	ArcSight™ Express Version 5.0 Patch 1	Added information for installing the Console, JRE update, and Patch 1
10/20/2010	ArcSight™ Express Version 5.0 Patch 1	Release Notes for AE v5.0 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/
Customer Forum	https://protect724.arcsight.com

Contents

- ArcSight Express, Version 5.0 Patch 1 5
 - Welcome to ArcSight Express 5
 - Purpose of this Release 5
 - Installation and Configuration 5
 - Installing the ArcSight Console 6
 - In this Release 6
 - Usage Notes 6
 - Adobe Flash Player Limitation 6
 - Using ssh Session to Upgrade 7
 - Upgrade-related Notes 7
 - Section 508 Compliance 8
 - Geographical Information Update 8
 - Vulnerability Updates 8
 - Issues Fixed in this Release 9
 - Open Issues in This Release 9

ArcSight Express, Version 5.0 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. 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 v5.0 Patch 1 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

- Upgrade to v5.0 Patch 1 is supported from v4.5 SP2 Patch 2, or v4.5 SP3. If you are upgrading from any other version of ESM, you are required to upgrade to either v4.5 SP2 Patch 2 or v4.5 SP3, before upgrading to v5.0 Patch 1.
- If you are on v4.5 SP2, make sure that you have the v4.5 SP2 Patch 2 installed before upgrading to v5.0 Patch 1.

Purpose of this Release

The purpose of this release is to:

- introduce an upgrade path for existing ArcSight Express customers to the latest release of ArcSight ESM. Please reference the What's New section in the *ESM v5.0 Release Notes* for a complete list of features introduced with v5.0.
- provide the latest JRE update

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.

Installing the ArcSight Console

Refer to the *ArcSight Express Configuration Guide* to install the v5.0 GA Console. After you have installed the v5.0 GA Console successfully, refer to the *ArcSight ESM v5.0 Patch 1 Release Notes* for instructions to install the JRE update and Patch 1.

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.

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, 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

Using an `ssh -X` session to upgrade ArcSight Express causes errors.

Instead of using `ssh -X` to upgrade ArcSight Express, run the upgrade in a simple `ssh` connection to the appliance.

Upgrade-related Notes

- Although the upgrade program does not prevent you from doing so, upgrading directly from v4.5 SP1 Patch 2 to v5.0 Patch 1 is not supported. If you are on v4.5 SP1 Patch 2 and would like to upgrade to v5.0 Patch 1, make sure you first upgrade to v4.5 SP2 Patch 2 before upgrading to v5.0 Patch 1.
- You will not be able to do two consecutive upgrades on the same day. For example, upgrading from v4.5 SP2 to v4.5 SP3, then upgrading to v5.0 Patch 1 cannot be done on the same day.

After doing one upgrade, wait until the execution of the next scheduled Partition Manager job before doing the next upgrade. This allows Partition Manager to create a new partition which allows the system to be recognized as upgraded to an intermediate version. Execution of the Partition Manager scheduled job can be ensured by letting the Manager from the first upgrade run for a day (24 hours). Do the next upgrade after a day.

- **For the ArcSight Express All-in-One appliance only:** You may use the ArcSight Express 5.0 Patch 1 upgrade to upgrade the ESM component in the ArcSight Express All-in-One appliance from 4.5 SP2 Patch 2. However, because ArcSight Express All-in-One uses a different directory structure for ESM Forwarding Connector (`/opt/arcsight/connector_esm`), the AE upgrade will overwrite the Logger Forwarding Connector directory which is in `/opt/arcsight/connector`. The following procedure describes how to save the existing directories and restore them after the upgrade:

- a** In the ArcSight Express All-in-One appliance, log in as root and stop the Logger connector:

```
# /opt/local/monit/bin/monit stop connector
```

- b** Stop the ESM connector:

```
# /opt/local/monit/bin/monit stop connector_esm
```

- c** Move the Connector directories so that the Logger connector is not accidentally upgraded:

```
# cd /opt/arcsight
```

```
# mv connector connector_logger
```

```
# mv connector_esm connector
```

- d** Run the ArcSight Express 5.0 Patch 1 upgrade over an ssh session with X-forwarding disabled (if you run it through out-of-band access or with X enabled, the upgrade will fail and may become unrecoverable):

```
# perl aeupdate-5.0.0.6521.1.pl
```

This is a silent upgrade. If you want to check the status, refer to the logs in the `/opt/updates` directory.

- e** After a successful upgrade, stop the connectors again and restore the connector directories:

```
# /opt/local/monit/bin/monit stop connector
# /opt/local/monit/bin/monit stop connector_esm
# cd /opt/arcsight
# mv connector connector_esm
# mv connector_logger connector
# /opt/local/monit/bin/monit start connector
# /opt/local/monit/bin/monit start connector_esm
```

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.

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20100901.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort Sourcefire SEU 367	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Enterasys Dragon IDS	Faultline, CVE, Nessus, CERT, MSSB
Cisco Secure IDS S512	Faultline, Bugtraq, CVE, Nessus
McAfee Intrushield	Faultline, CVE, MSSB
TippingPoint UnityOne DV8090	Faultline, Bugtraq, CVE, MSSB
Fortinet Fortigate	Bugtraq, MSSB
IBM/ISS SiteProtector	Faultline, Bugtraq, CVE, X-Force, MSSB, CERT
Symantec Endpoint Protection	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT
McAfee HIPS 7.0	Faultline, CVE, MSSB
FunkWerk (VarySys Technologies) PacketAlarm	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB

Issues Fixed in this Release

The following ArcSight Express specific issues were fixed in this release. For ESM related issues addressed in this release, refer to the *ArcSight ESM v5.0 Patch 1 Release Notes*. Also refer to the *ArcSight ESM v5.0 GA Release Notes* for v5.0 related information.

Number	Description
ESM-45857	<p>After upgrading to ESM v5.0 Patch 1 with IdentityView Express v1.1 SP1 installed, some IdentityView Express v1.1 SP1 resources show as invalid resources.</p> <p>To workaround this, edit the IdentityView Express v1.1 SP1 filter called "Built In Identities on IDM System" and remove the <code>setAction</code> local variable. This can be done before or after upgrade.</p>
ESM-46034	<p>Although the upgrade program does not prevent you from doing so, upgrading directly from v4.5 SP1 Patch 2 to v5.0 Patch 1 is not supported. If you are on v4.5 SP1 Patch 2 and would like to upgrade to v5.0 Patch 1, make sure you first upgrade to v4.5 SP2 Patch 2 before upgrading to v5.0 Patch 1.</p>

Open Issues in This Release

These open technical issues merit your review to avoid difficulties.

Number	Description
ESM-34779 TTP#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 where you import the Manager certificate using the Console wizard screen that prompts you to select your authentication type.</p> <p>Workaround: Restart the Console.</p>
ESM-34873 TTP#53977	<p>Space Based Retention: Occasionally you will not receive a warning email when free tablespace is under 5%.</p>
ESM-35370 TTP#55289	<p>If you start the wizard to configure ArcSight Database using the <code>./arcsight database pc</code> command, make sure to 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>
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> <pre>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>

Number	Description
ESM-35664 TTP#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> <p>Could not look up internet addresses for <hostname>.This will prevent GNOME from operating correctly.</p>
ESM-35565 TTP#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 harmless and can be safely ignored.</p>
ESM-41565 TTP#69272	<p>The upgrade installer does not check available disk space and fails if there is insufficient space.</p> <p>Workaround: Make sure you have at least 2GB disk space free before continuing with the patch installation.</p>
ESM-45903	<p>On the M7100 and M7200 machines you will see the following Java IOException</p> <p>Cannot run program "/usr/bin/tw_cli /c0 show all"</p> <p>after upgrading from v4.5 to v5.0 Patch 1. This exception does not affect the performance of the onboard Forwarding Connector and can be safely ignored.</p>
ESM-45937	<p>After applying v5.0 Patch 1, when you connect to ArcSight Express for the first time using the ESM 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 a fresh installation where you import the Manager certificate using the Console wizard screen that prompts you to select your authentication type.</p> <p>Workaround: Close, then re-open the Console.</p>