

Release Notes **ArcSight™ Express**

Version 4.5 SP3 Patch 2
Build 4.5.3.6152.2

December, 2010



Release Notes ArcSight™ Express, Version 4.5 SP3 Patch 2

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
12/29/10	ArcSight™ Express Version 4.5 SP3 Patch 2	Release Notes for this product version

Release Notes template version: 2.0.0

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/
Customer Forum	https://forum.arcsight.com

Contents

ArcSight Express, Version 4.5 SP3 Patch 2	1
Welcome to ArcSight Express	1
Purpose of this Patch	1
Usage Notes	2
Adobe Flash Player Limitation	2
Geographical Information Update	2
Vulnerability Updates	2
Installing ArcSight Express v4.5 SP3, Patch 2	3
Confirming a Successful Installation	4
Installing Patch 2 on ArcSight Console	5
Uninstalling the Patch	6
Rolling Back to the Previous Version	6
Issues Fixed in this Patch	9
Issues Fixed in v4.5 SP3 Patch 1	9
Installation and Upgrade	9
Issues Fixed in v4.5 SP3	9

ArcSight Express, Version 4.5 SP3 Patch 2

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.



Refer to the *ArcSight ESM v4.5 SP3, Patch 2 Release Notes* for information about ArcSight ESM open technical issues.

Refer to the *ArcSight Logger v4.5 Release Notes* for information about ArcSight Storage Appliance open technical issues.



- This patch is applicable only to ArcSight Express v4.5 SP3 and 4.5 SP3 Patch 1.
 - If you are upgrading ESM software from an older version of ArcSight Express, you are required to upgrade to all the interim versions, one at a time, before upgrading to v4.5 SP3, Patch 2.
-

Purpose of this Patch

This patch addresses:

- Customer requested and other issues
- Updates for geographical information and vulnerability mapping

Usage Notes

Note the following before installing this patch:

- Check the software build number on your ArcSight Express appliance by running the following from a command prompt.

```
rpm -q arcsight-express-manager
```
- After installing the patch, copy any Case customizations that you may have made to the Console, Manager and Web
`<ARCSIGHT_HOME>\i18n\common\label_strings.properties` and
`<ARCSIGHT_HOME>\i18n\common\resource_strings.properties` files from the backup of your previous installation. When you install the patch, configuration files are not merged from your previous installation.

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>).

Geographical Information Update

ArcSight Express contains recent geographical information used in graphic displays. The version is GeoIP-532_20101201.

Vulnerability Updates

This patch contains updated vulnerability mapping (December, 2010, Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 398 updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSSB
Enterasys Dragon IDS updated Faultline	CVE, Nessus, MSSB
Cisco Secure IDS S535 updated Faultline	CVE
McAfee Intrushield updated	Faultline, CVE
TippingPoint UnityOne DV8143 updated Faultline	Bugtraq, CVE, MSSB
Fortinet Fortigate updated	Bugtraq, MSSB
ISS SiteProtector Updated	Bugtraq, CVE, X-Force, MSSB
Symantec Endpoint Protection updated Faultline	Bugtraq, CVE, Nessus
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSKB, CERT, MSSB
FunkWerk (VarySys Technologies) PacketAlarm updated Faultline	Bugtraq, CVE, X-Force, Nessus, MSKB, MSSB

Installing ArcSight Express v4.5 SP3, Patch 2

To install the components on your ArcSight Express appliance:

- 1 Obtain and note the build number on your ArcSight Express Appliance and make a note of it. If you need to contact ArcSight Customer Support in future, you need to have your build number handy.

To check the software build number on your ArcSight Express appliance, run the following from a command prompt.

```
rpm -q arcsight-express-manager
```

If you see the output:

```
arcsight-express-manager-4.5.3-M6126
```

or

```
arcsight-express-manager-4.5.3-M6138
```

then you are on v4.5 SP3 or 4.5 SP3 Patch 1, respectively, and you can install this patch. Otherwise, you will need to first upgrade to v4.5 SP3 before proceeding any further.

- 2 Download the self-extracting upgrade file, `aeupdate_delta-4.5.3.xxxx.2.pl`, from the ArcSight Customer Support web site. The `xxxx` in the file name stands for the build number.
- 3 If you download the file(s) to a system other than the ArcSight Express appliance that you want to upgrade, move the file(s) over to the ArcSight Express appliance using the `scp` command. For example, from your local machine where the file(s) are located, run:

```
scp aeupdate_delta-4.5.3.xxxx.2.pl root@<hostname>:/root
```

- 4 You can perform the rest of the steps either directly on the ArcSight Express machine or remotely using `ssh`. To use `ssh`, open a shell window by running:

```
ssh root@<hostname>.<domain>
```



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

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

- 5 Verify the integrity of the update file you have downloaded:
 - a Open a browser and go to the ArcSight Download Center.
 - b Click 'Estimated Times and Details' link in the box from which you downloaded your executable file.
 - c In the Download Details window, verify the MD5 Signature.
- 6 For customers upgrading their environment from v4.5 SP3, we recommend that you copy the following file to a secure location before installing the patch.

```
/opt/arcsight/db.preUpgradeBackup/arcsight.dmp
```



When you upgraded to v4.5 SP3, an `arcsight.dmp` file (containing your base ESM installation) was created in the `/opt/arcsight/db.preUpgradeBackup` directory. If, for any reason, you have to roll back to that installation after or during an upgrade, ArcSight recommends that you first copy the `arcsight.dmp` file to a secure location. This allows you to restore that data, if needed.

The `arcsight.dmp` file is overwritten with all subsequent upgrades.

7 Run the self-extracting install file:

```
perl aeupdate_delta-4.5.3.xxxx.2.pl
```

- ◆ During the upgrade, the existing software components are backed up to the following locations:

- `/opt/arcsight/db.preUpgradeBackup`
- `/opt/arcsight/manager.preUpgradeBackup`
- `/opt/arcsight/web.preUpgradeBackup`



If you do multiple upgrades, the `preUpgradeBackup` files are overwritten each time. For example, if you are on v4.5 GA and upgrade to v4.5 SP2, backup files are created for the v4.5 GA installation. But if you further upgrade from v4.5 SP2 to v4.5 SP3, Patch 2, the v4.5 GA backup files are overwritten with the v4.5 SP3 backup files.

Consequently, rollback to v4.5 GA version is not possible because backup files cannot be retrieved.

- ◆ The `aeupdate_delta-4.5.3.xxxx.2.pl` file extracts itself into a subdirectory within `/opt/updates` directory and automatically upgrades the existing RPMs.
- ◆ The following log files for the upgrade are placed in the `/opt/updates` directory.
 - `*.res` - shows the result of the operation, such as success, error, or reboot
 - `*.log` - records the details of the upgrade process

where `*` stands for the name of the self-extracting perl file.

- ◆ Make sure to copy any Case customizations that you may have made to the Manager and Web's
`<ARCSIGHT_HOME>\i18n\common\label_strings.properties` and
`<ARCSIGHT_HOME>\i18n\common\resource_strings.properties` files from the backup of your previous installation. When you install the patch, configuration files are not merged from your previous installation.

Confirming a Successful Installation

To make sure that your upgrade completed, run:

```
rpm -qa | grep express | sort
```

You should see the following packages listed where `xxxx` stands for the patch build number (as shown within the title of the document).

`arcsight-express-db-4.5.3-Mxxxx`
`arcsight-express-manager-4.5.3-Mxxxx`
`arcsight-express-web-4.5.3-Mxxxx`

You have installed ArcSight Express v4.5 SP3, Patch 2.



Note

An incomplete or aborted install might show some packages with the new version number, while others have the original (pre-patch) version number, depending upon where the component patch halted.



Caution

Make sure that you have obtained the new license file from ArcSight Customer Support and updated your appliance with it.

Be sure to upgrade your existing Console, as described in the following section.

Installing Patch 2 on ArcSight Console

This section describes how to install or uninstall v4.5 SP3, Patch 2 for ArcSight Console on Windows platforms.

To Install



Note

Before you install the patch, verify that the Console's `ARCSIGHT_HOME` and any of its subdirectories are not being accessed by open shells on your system.

If for any reason you need to re-install the patch, run the patch uninstaller before installing the patch again.

- 1 Exit the ArcSight Console.
- 2 Back up the Console `current` directory by making a copy. Place the copy in a readily accessible location. This is a precautionary measure so you can restore the original state, if necessary.



Caution

ArcSight recommends that you do not simply rename files and leave them in the same directory. Java reads all the files present, regardless of renaming, and can pick up old code inadvertently, causing undesirable results.

- 3 Download the Console's executable file, `Patch-4.5.3.xxxx.2-Console-Win.exe`, from the ArcSight Software download web site. The `xxxx` in the file name represents the build number.
- 4 Double-click `Patch-4.5.3.xxxx.2-Console-Win.exe`.

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing `ARCSIGHT_HOME` for your v4.5 SP3 Console installation in the text box provided or navigate to the location by clicking **Choose...**

If you want to restore the installer-provided default location, click **Restore Default Folder**.

- 7 Click **Next**.

- 8 Choose a Shortcut location by clicking the appropriate radio button and click **Next**.
- 9 Check the pre-installation summary to verify that all the locations listed are correct and that you have enough disk space to install this patch.
- 10 Click **Install**.
- 11 Click **Done** on the Install Complete screen.

Uninstalling the Patch

If needed, use the procedure below to roll back this patch installation.



Before you begin to uninstall, verify that the Console's [ARCSIGHT_HOME](#) and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Exit the ArcSight Console if it is running.
- 2 Double-click the icon you created for the uninstaller when installing the Console. For example, if you created an uninstaller icon on your desktop, double-click that icon.
 - ◆ Or, if you created a link in the Start menu, go to
Start->All Programs->ArcSight Console SP3 Patch2-> Uninstall ArcSight Console 4.5 SP3 Patch 2
 - ◆ Or run the following from the Console
`<ARCSIGHT_HOME>\current\UninstallerDataSP3Patch2` directory.
`Uninstall_ArcSight_Console_Patch.exe`
- 3 Click **Done** on the Uninstall Complete screen.

Rolling Back to the Previous Version

If you encounter a problem when installing this patch you can roll back the software to the base installation which existed on your ArcSight Express appliance before you started installing the patch. You can roll back only the Database, Manager, and Web.



- If you run into serious issues when upgrading, ArcSight recommends that you contact ArcSight Customer Support **before** you roll back your upgrade.
 - When you upgraded to v4.5 SP3, an `arcsight.dmp` file (containing your base ESM installation) was created in the `/opt/arcsight/db.preUpgradeBackup` directory. If, for any reason, you have to roll back to your original installation after or during an upgrade, ArcSight recommends that you first copy the `arcsight.dmp` file to a secure location. This allows you to restore your original data, if needed.
 - The `arcsight.dmp` file is overwritten with all subsequent upgrades.
-

If the patch installation fails, file an ArcSight Customer Support ticket and provide the installation logs. You have the option to repair the incomplete patch installation manually with the help of ArcSight Support, or you can roll back to the previous version.

To rollback to the previous version of the software:

- 1 Make sure you are logged in as user "root".
- 2 Stop ArcSight Manager:

```
/etc/init.d/arcsight_manager stop
```

3 Stop ArcSight Web:

```
/etc/init.d/arcsight_web stop
```

4 Delete the ArcSight Express components by running:

```
rpm -e --nodeps arcsight-express-web-4.5.3-Mxxxx
```

```
rpm -e --nodeps arcsight-express-manager-4.5.3-Mxxxx
```

```
rpm -e --nodeps arcsight-express-db-4.5.3-Mxxxx
```

Where **xxxx** represents a digit in the build number.

The above commands delete the ArcSight Express files. You will see warning(s) similar to this:

```
warning: /opt/arcsight/manager/jre/lib/security/cacerts saved
as /opt/arcsight/manager/jre/lib/security/cacerts.rpmsave
```

If the earlier upgrade failed to complete, an error message may appear stating that one or more of the packages is not installed.

5 Delete the remaining files under `/opt/arcsight/db`, `/opt/arcsight/manager`, `/opt/arcsight/web` (for example, the log files, `.config` file(s), and other dynamically created files):

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

```
rm -rf web manager db
```

6 Restore the backup versions of each component (Database, Manager, and Web):



If `web.preUpgradeBackup.01`, `db.preUpgradeBackup.01` or `manager.preUpgradeBackup.01` already exists, delete the folders before proceeding any further.

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

```
mv web.preUpgradeBackup web.preUpgradeBackup.01
```

```
mv manager.preUpgradeBackup manager.preUpgradeBackup.01
```

```
mv db.preUpgradeBackup db.preUpgradeBackup.01
```

```
cp -prd web.preUpgradeBackup.01 web
```

```
cp -prd manager.preUpgradeBackup.01 manager
```

```
cp -prd db.preUpgradeBackup.01 db
```

7 Check whether you need to download and extract your previous update bundle. "**XXXX**" represents the previous installation build number (e.g., [6126](#) or [6138](#). If both exist, use the larger number.)

```
cd /opt/updates/aeupdate-4.5.3.xxxx.x/RPMS
```

If the directory exists, you do not need to do the download and extraction. Go to [Step 10](#).

-
- 8 Download the update bundle of your previous installation, `aeupdate-4.5.3.xxxx.x.pl`, from ArcSight Support download web site.
 - 9 Extract the contents of this file by running the following command (be sure to include the `-n` option at the end:

```
perl aeupdate-4.5.3.xxxx.x.pl -n
```

This creates the `/opt/updates/aeupdate-4.5.3.xxxx.x/RPMS` directory.

- 10 Go to the RPMS directory:

```
cd /opt/updates/aeupdate-4.5.3.xxxx.x/RPMS
```

```
mkdir /root/rpms.xxx
```

```
cp arcsight-express-*.rpm /root/rpms.xxx
```

```
cd /root/rpms.xxx
```

- 11 Synchronize the RPM database with the file set that is currently on your local disk from the directory where you downloaded it. (In the example above, it would be `cd /root/rpms.xxx/`). If all your components are in the same directory, run:

```
rpm -i --justdb --nodeps --noscripts --notriggers *.rpm
```

If you copied your RPM files to multiple locations, run the command for each component individually from their respective locations as follows:

Database:

```
rpm -i --justdb --nodeps --noscripts --notriggers arcsight-express-db-4.5.3-Mxxxx.x86_64.rpm
```

Manager:

```
rpm -i --justdb --nodeps --noscripts --notriggers arcsight-express-manager-4.5.3-Mxxxx.x86_64.rpm
```

Web:

```
rpm -i --justdb --nodeps --noscripts --notriggers arcsight-express-web-4.5.3-Mxxxx.x86_64.rpm
```

- 12 Start the Manager:

```
/etc/init.d/arcsight_manager start
```

- 13 Start the Web:

```
/etc/init.d/arcsight_web start
```

Issues Fixed in this Patch

There were no issues specific to ArcSight Express that were fixed in this release.

For ESM-related issues addressed in this release, refer to the *ArcSight ESM v4.5 SP3 Patch 2 Release Notes*.

Issues Fixed in v4.5 SP3 Patch 1

For ESM-related issues addressed in Patch 1, refer to the *ArcSight ESM v4.5 SP3 Patch 1 Release Notes*.

The following issue was addressed in Patch 1.

Installation and Upgrade

Number	Description
ESM-41565 TTP#69272	The upgrade installer did not check available disk space and failed if there was not enough. Now the installer confirms whether the system has enough disk space to apply the patch. If the space requirement is not met, the user gets a message to that effect and the upgrade cannot continue until the disk space requirement is satisfied.

Issues Fixed in v4.5 SP3

There were no issues specific to ArcSight Express that were fixed in the SP3 release.

For ESM-related issues addressed in this release, refer to the *ArcSight ESM v4.5 SP3 Release Notes*.
