

Patch Release Notes **ArcSight™ Express**

Version 4.5 SP2, Patch 1
Build 4.5.2.6088.1

March 17, 2010



Release Notes ArcSight™ Express, Version 4.5 SP2, Patch 1

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
03/17/10	ArcSight™ Express Version 4.5 SP2, Patch 1	Updated Release Notes to include SP2, Patch 1 information.

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://forum.arcsight.com

Contents

ArcSight Express, Version 4.5 SP2, Patch 1	1
Welcome to ArcSight Express	1
Purpose of this Patch	1
Usage Notes	1
Using ssh Session to Install or Run First Boot Wizard	2
Adobe Flash Player Limitation	2
Geographical Information Update	2
Vulnerability Updates	2
Installing ArcSight Express v4.5 SP2, Patch 1	3
Confirming a successful installation	4
Installing Patch 1 on ArcSight Console	5
Uninstalling the Patch	6
Rolling Back to the Previous Version	6
Issues Fixed in this Patch	8
Open Issues in This Patch	9

ArcSight Express, Version 4.5 SP2, 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.



Note

Refer to the *ArcSight ESM v4.5 SP2, 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

- This patch is applicable only to ArcSight Express v4.5, SP2.
- 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 SP2, Patch 1.

Purpose of this Patch

This patch addresses:

- Customer requested and other issues
- Updates for geographical information and vulnerability mapping
- Delivery of Oracle January CPU

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>\il8n\common\label_strings.properties` and
`<ARCSIGHT_HOME>\il8n\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.

Using ssh Session to Install or Run First Boot Wizard

Using an `ssh -X` session to either install ArcSight Express or run First Boot Wizard causes errors and the FBW does not complete.

Workaround: Instead of using `ssh -X` to run FBW or install ArcSight Express, use `ssh` to connect to the appliance and set your `DISPLAY` environment variable to point to a valid X11 display.

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_20100201**.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU 253	Bugtraq, CVE, X-Force, MSSB
Enterasys Dragon IDS	Bugtraq, CVE, Nessus, CAN, MSSB
Cisco Secure IDS S424	Bugtraq, CVE
McAfee Intrushield	CVE, MSSB
TippingPoint UnityOne DV7755	Bugtraq, CVE, X-Force, CERT, MSKB, MSSB
Fortinet Fortigate	Bugtraq, CVE, X-Force, MSSB
ISS SiteProtector	Bugtraq, CVE, X-Force, MSKB, MSSB, CERT
Symantec Endpoint Protection	Bugtraq, CVE
Radware DefensePro	CVE
FunkWerk (VarySys Technologies) PacketAlarm	Bugtraq, CVE, X-Force, Nessus, MSSB, MSKB, CERT

Installing ArcSight Express v4.5 SP2, Patch 1

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-4.5.2-M6076
```

then you are on v4.5 SP2 and you can install this patch. Otherwise, you will need to first upgrade to v4.5 SP2 before proceeding any further.

- 2 Download the self-extracting upgrade file, `aeupdate_delta-4.5.2.xxxx.x.pl` and, optionally, its checksum file, `aeupdate_delta-4.5.2.xxxx.x.pl.md5`, 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-4.5.2.xxxx.x.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 downloaded to make sure that it was not truncated or corrupted during the download. Run:

```
md5sum -c aeupdate_delta-4.5.2.xxxx.x.pl.md5
```

- 6 Before installing the patch, we recommend that you copy the following file to a secure location:

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



When you upgraded to 4.5 SP2, 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.

7 Run the self-extracting install file:

```
perl aeupdate_delta-4.5.2.xxxx.x.pl
```

- ◆ Before the upgrade process begins, the existing software components are backed up to the following locations:

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



Note

If you do multiple upgrades, the `preUpgradeBackup` files are overwritten each time you do an upgrade. 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 SP2, Patch 1, the v4.5 GA backup files are overwritten with the v4.5 SP2 backup files.

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

- ◆ The `aeupdate_delta-4.5.2.xxxx.x.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-4.5.2-Mxxxx  
arcsight-express-manager-4.5.2-Mxxxx  
arcsight-express-web-4.5.2-Mxxxx
```



Note

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



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

You have installed ArcSight Express v4.5 SP2, Patch 1.

Be sure to upgrade your existing Console. See [Installing Patch 1 on ArcSight Console](#) below.

Installing Patch 1 on ArcSight Console

This section describes how to install or uninstall v4.5 SP2, Patch 1 for ArcSight Console on Windows platforms.

To Install



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.



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-4.5.2.xxxx.1-Console-Win.exe](#), from the ArcSight Software download website. The [xxxx](#) in the file name represents the build number.
- 4 Double-click [Patch-4.5.2.xxxx.1-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 SP2 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.



Note

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 SP2 Patch1-> Uninstall ArcSight Console 4.5 SP2 Patch 1
 - ◆ Or run the following from the Console
`<ARCSIGHT_HOME>\current\UninstallerDataSP2Patch1 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.



Caution

- 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 4.5 SP2, 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-4.5.2-Mxxxx
```

```
rpm -e --nodeps arcsight-express-manager-4.5.2-Mxxxx
```

```
rpm -e --nodeps arcsight-express-db-4.5.2-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.rpm.save
```

If the installation fails before it completes, an error message appears 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 v4.5.2 versions of each component (Database, Manager, and Web):

```
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 the 4.5 SP2 update bundle:

```
cd /opt/updates/aeupdate-4.5.2.6076.0/RPMS
```

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

8 Download the 4.5 SP2 update bundle, `aeupdate-4.5.2.6076.0.p1`, from ArcSight Support download website.

-
- 9** Extract the contents of this file by running the following command (be sure to include the `-n` option at the end:

```
perl aeupdate-4.5.2.6076.0.pl -n
```

This creates the `/opt/updates/aeupdate-4.5.2.6076.0/RPMS` directory.

- 10** Go to the RPMS directory:

```
cd /opt/updates/aeupdate-4.5.2.6076.0/RPMS
```

```
mkdir /root/rpms.452
```

```
cp arcsight-express-*.rpm /root/rpms.452
```

```
cd /root/rpms.452
```

- 11** Synchronize the RPM database with the fileset that is currently on your local disk from the directory where you downloaded it. (In the example above, it would be `cd /root/rpms.452/`). 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-4.5.2-M6076.x86_64.rpm
```

Manager:

```
rpm -i --justdb --nodeps --noscripts --notriggers arcsight-express-manager-4.5.2-M6076.x86_64.rpm
```

Web:

```
rpm -i --justdb --nodeps --noscripts --notriggers arcsight-express-web-4.5.2-M6076.x86_64.rpm
```

- 12** Start the Manager:

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

- 13** Start the Web:

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

Make sure to move or rename the `/opt/updates` directory.

Issues Fixed in this Patch

There are no fixed issues for this patch.

For ESM related issues addressed in Patch 1, refer to the *ArcSight ESM v4.5 SP2, Patch 1 Release Notes*.

For ArcSight Express issues addressed in v4.5 SP2, refer to the *ArcSight Express v4.5 SP2 Release Notes*.



These release notes document issues specific to ArcSight Express v4.5 SP2, Patch 1.

Open Issues in This Patch

There following issues merit your attention.

Number	Description
58665	<p>If, after running ESM for several weeks, the Manager appears to hang and you receive the following error message</p> <pre>unable to extend temp segment by 32 in tablespace TEMP</pre> <p>this may be due to unbounded growth of a TEMP file (<code>/home/oracle/OraHome10g/oradata/Arcsight/temp01.dbf</code>) which currently has no set size limitation.</p> <p>The following workaround sets this limitation and limits the TEMP file growth to a maximum of 8G.</p> <p>Workaround:</p> <ol style="list-style-type: none">1 Stop all ESM components (ArcSight Web, ArcSight Manager, and the database).2 Connect to sqlplus while logged in as a system user and execute the following command. <pre>alter database tempfile '/home/oracle/OraHome10g/oradata/arcsight/temp01.dbf' autoextend on MAXSIZE 8000M;</pre> <ol style="list-style-type: none">3 Exit from sqlplus and restart all the ESM components.
65294	<p>The ArcSight Express “What’s New” window fails to display the ArcSight Web and Network Model Wizard icons.</p>
