

Release Notes **ArcSight™ Express**

Version 5.0 SP2 Patch 3
Build 5.0.2.6904.3

June 1, 2012



Release Notes ArcSight™ Express Version 5.0 SP2 Patch 3

Copyright © 2012 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

ArcSight Express, Version 5.0 SP2 Patch 3	5
Welcome to ArcSight Express	5
Purpose of this Release	5
Section 508 Compliance	5
Usage Notes	5
Copy Case Customizations	5
In this Release	6
Installing ArcSight Express v5.0 SP2 Patch 3	6
Series M7100, M7200, and M7400 Appliances	6
Confirming a Successful Installation	8
Rolling Back to the Previous Version	9
Installing Patch 3 on ArcSight Console	11
To Install the Patch	11
To Install the Patch on an Mac	12
To Uninstall the Patch	13
Issues Fixed in this Release	14
Open Issues in this Patch	14
Database	14

ArcSight Express, Version 5.0 SP2 Patch 3

Welcome to ArcSight Express

These release notes describe how to apply this patch release of ArcSight Express appliance. Instructions are included for each component, as well as other information about recent changes and open and closed issues. This patch is *not* for ArcSight Express All-in-One appliance.

Refer to the *ArcSight ESM v5.0 SP2 Patch 3 Release Notes* for information about ArcSight ESM open technical issues, geographical information update, and vulnerability updates.

Refer to the *ArcSight Logger v5.2 Release Notes* for information about ArcSight Storage appliance open technical issues.

Upgrade to v5.0 SP2 Patch 3 is supported from v5.0 SP2 Patch 2. If you are upgrading from any other version of ESM, first upgrade to v5.0 SP2 Patch 2, so you can then upgrade to v5.0 SP2 Patch 3.

Purpose of this Release

This patch:

- Introduces an upgrade path for existing ArcSight Express appliance customers to the latest release of ArcSight ESM.
- Provides updates for geographical information and vulnerability mapping.
- Provides certification with the April 2012 Oracle PSU.

See the *ESM v5.0 SP2 Patch 3 Release Notes* for information about v5.0 SP2 Patch 3.

Section 508 Compliance

HP recognizes the importance of accessibility as a product initiative. To that end, HP is making advances in the area of accessibility in its product lines.

Usage Notes

Copy Case Customizations

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.

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:

- **Manager** provides correlation and analytics. It manages, cross-correlates, filters, and processes all security events in your enterprise. The Manager includes a Cross-Correlation Engine, Connector Data Manager, tracking and resolution functions, and analytics and reporting capabilities. The 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.
- **Forwarding Connector** transports events from the ArcSight Express appliance to the ArcSight Storage appliance.

In addition to these components, the ArcSight Storage appliance also contains 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.

Installing ArcSight Express v5.0 SP2 Patch 3

Series M7100, M7200, and M7400 Appliances

The upgrade to v5.0 SP2 Patch 3 is supported from v5.0 SP2 Patch 2 on M7100, M7200, and M7400 appliances. 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 HP 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-5.0.2-Mxxxx
```

then you are on v5.0 SP2 Patch 2 and you can install this patch. Otherwise, you will need to first upgrade to v5.0 SP2 Patch 2 before proceeding any further.

- 2 Download the self-extracting upgrade file, `aeupdate_delta-5.0.2.xxxx.3.pl`, from the Downloads tab of the HP SSO site, where `xxxx` is the build number.
- 3 If you download the file to a system other than the ArcSight Express appliance that you want to upgrade, move the file to the ArcSight Express appliance using the `scp` command. For example, from your local machine where the file are located, run:

```
scp aeupdate_delta-5.0.2.xxxx.3.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 installer in a simple `ssh` connection to the appliance.

- 5 We recommend that you copy the following file to a secure location before installing the patch.

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



On M7200 and M7100, when you upgraded to v5.0 SP2 Patch 2, 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 during or after an upgrade, HP 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.

- 6 Run the self-extracting install file:

```
perl aeupdate_delta-5.0.2.xxxx.3.pl
```

(Wherever you see `.pl`, the second character is a lowercase L, not the numeral one.) During upgrade, the existing software components are backed up to these locations:

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



For multiple upgrades, the `preUpgradeBackup` files are overwritten each time. For example, if you are on v5.0 GA and upgrade to v5.0 SP1 Patch 3, backup files are created for the v5.0 GA installation. But if you further upgrade from v5.0 SP1 to v5.0 SP2 Patch 2, the v5.0 SP1 backup files are overwritten with the v5.0 SP2 P2 backup files.

Consequently, rollback to v5.0 SP1 version is not possible because backup files cannot be retrieved.

- ◆ The `aeupdate_delta-5.0.2.xxxx.3.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 processwhere `*` 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 was 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-5.0.2-Mxxxx
arcsight-express-manager-5.0.2-Mxxxx
arcsight-express-web-5.0.2-Mxxxx
```



An incomplete or aborted installation 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.

For M7400, M7200, and M7100 customers, make sure the Oracle PSU was installed correctly, as follows:

- 1 As 'root' user, execute the following command (no line break):

```
sudo -u oracle /home/oracle/OraHome10g/OPatch/opatch
lsinventory | grep "Patch<value>"
```

For M7200 and M7100 `<value> = s*12879933`.
For M7400, `<value> = s*13696224`.

- 2 For a successfully completed patch, you will see,

```
Patch <value> : applied on <date>
```

If you do not see the above output, please contact HP Customer support.

You have installed ArcSight Express v5.0 SP2 Patch 3.



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

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

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, contact HP Customer Support *before* you roll back your upgrade.
- When you upgraded to v5.0 SP2 Patch 2, an `arcsight.dmp` file (containing your base ESM installation) was created in the `/opt/arcsight/db.preUpgradeBackup` directory. If you have to roll back to your original installation after or during an upgrade, HP recommends that you first copy the `arcsight.dmp` file to a secure location. This allows you to restore your original data, if necessary.
- The `arcsight.dmp` file is overwritten with all subsequent upgrades.

If the patch installation fails, file an HP Customer Support ticket and provide the installation logs. You have the option to repair the incomplete patch installation manually with the help of HP 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 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-5.0.2-Mxxxx
```

```
rpm -e --nodeps arcsight-express-manager-5.0.2-Mxxxx
```

```
rpm -e --nodeps arcsight-express-db-5.0.2-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.rpmsave
```

If the earlier upgrade failed to complete, an error message might 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.

```
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 (such as 6846. If two numbers exist, use the larger number).

```
cd /opt/updates/aeupdate-5.0.2.xxxx.2/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 from HP SSO Support site.

`aeupdate-5.0.2.xxxx.2.pl`

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

```
perl aeupdate-5.0.2.xxxx.2.pl -n
```

This command creates the `/opt/updates/aeupdate-5.0.2.xxxx.2/RPMS` directory.

- 10** Execute the following commands:

```
cd /opt/updates/aeupdate-5.0.2.xxxx.2/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 arcsight-express-*.rpm
```

- 12** Start the Manager:

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

- 13** Start the Web:

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

Installing Patch 3 on ArcSight Console

This section describes how to install or uninstall the v5.0 SP2 Patch 3 for ArcSight Console for M7100, M7200, and M7400 appliances. Install the Console on other computers in your network, but not on the appliance. Apply the patch to the Manager on the appliance first. The console and manager need to be at the same version level.

To Install the Patch



- Before you install the patch, verify that the Console's `<ARCSIGHT_HOME>` and any of its subdirectories are not being accessed by any open shells on your system.
- If you need to reinstall the patch, run the patch uninstaller before installing the patch again.
- If your ArcSight Console is on 5.0 SP1 Patch 3 for Windows environments, you must first upgrade it to v5.0 SP2, then apply this v5.0 SP2 Patch 3 for the Console. For instructions about how to upgrade to the v5.0 SP2 ArcSight Console, see *Upgrading ArcSight ESM v5.0 GA or v5.0 SP1 to v5.0 SP2* ([ESM_Upgrading50GAor50Patch1To50SP2.pdf](#)) available from the Download tab of the HP SSO site (<http://support.openview.hp.com>)

If you are installing the ArcSight Console on a Mac, go to ["To Install the Patch on an Mac" on page 12](#).

- 1 Exit the ArcSight Console.
- 2 Back up the Console directory (for example, `/home/arcsight/console/current`) 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.



HP 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 executable file specific to your platform from the Download tab of the HP SSO site (<http://support.openview.hp.com>). (In the following file names, `xxxx` represents the build number.)

- ◆ `Patch-5.0.2.xxxx.3-Console-Win.exe`
- ◆ `Patch-5.0.2.xxxx.3-Console-Linux.bin`

- 4 Run one of the following executables specific to your platform:

◆ **Windows:**

Double-click `Patch-5.0.2.xxxx.3-Console-Win.exe`

◆ **Linux:**

Verify that you are logged in as the ArcSight user, and then run the following command:

```
./Patch-5.0.2.xxxx.3-Console-Linux.bin
```

To install in Console mode, run the following command from the shell prompt and then follow the instructions in the window:

```
./Patch-5.0.2.xxxx.3-Console-Linux.bin -i console
```

The installer launches the Introduction window.

- 5 Read the instructions provided and click **Next**.
- 6 Enter the location of your existing <ARCSIGHT_HOME> directory for your v5.0 SP2 Patch 1 Console installation in the text box provided or navigate to the location by clicking **Choose...**

To restore the installer-provided default location, click **Restore Default Folder**.
- 7 Click **Next**.
- 8 Choose a Link Location (Solaris and Linux) or Shortcut location (Windows) 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.

To Install the Patch on an Mac

The patch installer download and run procedure is slightly different on the Mac than on the other supported platforms.

- 1 Exit the ArcSight Console.
- 2 Back up the Console directory (for example, `/home/arcsight/console/current`) 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.
- 3 Delete the existing Console directory after you have made a copy elsewhere. (This action uninstalls the Console.)



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.

- 4 Download the file `Patch-5.0.2.xxxx.3-Console-MacOSX.zip` (where `xxxx` represents the build number) into the directory in which the Console is installed (for example, `/home/arcsight/console/current`). Use the number that matches the specific patch number at the top of this document.



The patch installer file (that shows as a **ZIP** file on the download site) is downloaded as `Patch-5.0.2.xxxx.3-Console-MacOSX.app` on the Mac. A single or double-click on this **APP** file launches the patch installer, depending on how you have set these options. You do not need to “extract” or “unzip” the file when it downloads as an **APP** file.

- 5 Launch the patch installer by double-clicking the `ArcSightConsolePatch` file.

- 6 Follow the steps on the patch install wizard, providing the information as prompted:
 - ◆ Choose the location where you want to install the patch. Browse to the same the location of your existing `<ARCSIGHT_HOME>` directory for your v5.0 SP2 Patch 1 Console installation.
 - ◆ Choose an alias location for the Console application (or opt to not use aliases). An alias is the same as a link location on UNIX systems or a shortcut location on Windows systems.
- 7 Click **Next**.
- 8 Verify your settings and click **Install**.

To Uninstall 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>` directory and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Exit the ArcSight Console.
- 2 Run the uninstaller program:

Windows:

- ◆ 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.
- ◆ If you created a link in the Start menu, click
Start->ArcSight Console SP2Patch3-> Uninstall ArcSight Console 5.0 SP2Patch3

- ◆ Or, run the following .exe from the Console's `<ARCSIGHT_HOME>\current\UninstallerDataSP2Patch3` directory:
`Uninstall_ArcSight_Console_Patch.exe`

Linux:

- ◆ From the directory where you created the links when installing the Console (your home directory or some other location), run:
`./Uninstall_ArcSight_Console_5.0_SP2Patch3`
- ◆ Or, to uninstall using Console mode, run:
`./Uninstall_ArcSight_Console_5.0_SP2Patch3 -i console`
- ◆ If you did not create a link, execute the command from the Console's `<ARCSIGHT_HOME>/current/UninstallerDataSP2Patch3` directory:
`./Uninstall_ArcSight_Console_Patch`

On a Mac:

- ◆ From the directory where you created the links when installing the Console, run:
`Uninstall_ArcSight_Console_5.0_SP2Patch3`

- ◆ From the Console's
`<ARCSIGHT_HOME>/current/UninstallerDataSP2Patch3` directory, run:
`Uninstall_ArcSight_Console_5.0_SP2Patch3`

- 3 Click **Done** on the Uninstall Complete screen.

Issues Fixed in this Release

For ESM related issues addressed in this release, see the *ArcSight ESM v5.0 SP2 Patch 3 Release Notes*.

Open Issues in this Patch

This release contains the following open issues.

Database

Issue	Description
ESM-49726	<p>On ArcSight Express, the following report does not display results: /All Reports/Deprecated/Cache History by Connector</p> <p>Workaround</p> <p>Since '/All Reports/Deprecated/Cache History by Connector' is deprecated, you are advised to use '/All Reports/Arcsight Administrator/Connectors/Caches/Cache History by Connectors,' instead.</p> <p>Create a copy of the Query '/All Queries/Arcsight Administrator/Connectors/Caches/Cache History by Connectors'</p> <p>Edit the report '/All Reports/Arcsight Administrator/Connectors/Caches/Cache History by Connectors' to use the new copy of the Query.</p>
ESM-48952	<p>There are potential partition manager issues, which include reserve partitions not being created and out of tablespace warnings:</p> <p>To resolve these issues, make sure your Oracle I/O Transfer speed is greater than 4096 bytes per millisecond, the default value at installation. The function is supposed to automatically increase the speed. If the value does not increase, please contact HP Support. Refer to the KCS article, "Resetting Oracle I/O Transfer Speed," available on the HP SSO web site.</p>