

# Release Notes

---

ArcSight Express 4.0  
Patch 1

February 26, 2015



Copyright © 2015 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.hpenterprisesecurity.com/copyright>

#### Contact Information

---

<b>Phone</b>	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="http://softwaresupport.hp.com">http://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.hp.com">https://protect724.hp.com</a>

---

#### Revision History

---

<b>Date</b>	<b>Product Version</b>	<b>Description</b>
02/26/2015	ArcSight Express 4.0 Patch 1	Release Notes for ArcSight Express 4.0 Patch 1.

---

# Contents

---

<b>ArcSight Express 4.0 Patch 1 .....</b>	<b>5</b>
ArcSight Express 4.0 Patch 1 .....	5
Purpose of this Patch .....	5
Usage Notes for this Patch .....	6
Upgrade to Latest Connector Versions .....	6
Section 508 Compliance .....	6
Geographical Information Update .....	6
Vulnerability Updates .....	6
Installing ArcSight Express 4.0 Patch 1 .....	7
Verify AE 4.0 Patch 1 Files .....	7
ArcSight Express Main Component Suite .....	8
ArcSight Console .....	10
Issues Fixed in this Patch .....	13
Analytics .....	13
ArcSight Console .....	14
ArcSight Database .....	14
ArcSight Manager .....	14
Installation and Upgrade .....	15
Open Issues in this Patch .....	15
Installation and Upgrade .....	15
Connectors .....	16
Open and Closed Issues in ArcSight Express 4.0 .....	17



# ArcSight Express 4.0 Patch 1

---

## ArcSight Express 4.0 Patch 1

These release notes describe how to apply this patch release of ArcSight Express. Instructions are included for each component, as well as other information about recent changes and open and closed issues.

This patch is for ArcSight Express 4.0. To set up a new ArcSight Express 4.0 installation, refer to the ArcSight Express Installation and Configuration Guide.

The build number for the ArcSight Express suite for this patch is 1361

The build number for the ArcSight Console for this patch is 1933.1.

After you have installed ArcSight Express 4.0, follow the instructions in ["Installing ArcSight Express 4.0 Patch 1" on page 7](#) of these release notes to apply Patch 1.

## Purpose of this Patch

This patch:

- Addresses critical issues in ArcSight Express 4.0.
- Provides updates for geographical information and vulnerability mapping.
- Upgrades JRE version to 1.6.0\_65.
- Upgrades the tzdata version to tzdata2014f.
- Adds certification of Red Hat Enterprise Linux 6.5 (64-bit) for ArcSight Express Patch 1.

HP recommends that you upgrade your operating system from Red Hat Linux 6.2 to 6.5. Download the operating system upgrade script and technical note from HP SSO. Perform the operating system upgrade only after you have successfully upgraded your ArcSight Express installation to 4.0 Patch 1. See the Upgrade RHEL 6.2 to RHEL 6.5 for ArcSight Express Appliance Technical Note for details.

- Adds certification of CentOS Linux 6.5 (64-bit) for ArcSight Express VA Patch 1.  
HP recommends that you upgrade your operating system from CentOS Linux 6.2 to 6.5. Download the operating system upgrade script and technical note from HP SSO. Perform the operating system upgrade only after you have successfully upgraded your ArcSight Express VA installation to 4.0 Patch 1. See the Upgrade CentOS 6.2 to CentOS 6.5 for ArcSight Express Virtual Appliance Technical Note for details.
- Under certain loads, an unstable condition can on occasion arise that leads to a Signal 11 occurrence. This patch provides a significant improvement to reduce the likelihood of a Signal 11 condition.
- Provides the POODLE SSL fix

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit that takes advantage of Internet and

security software clients' fallback to SSL 3.0. See <http://en.wikipedia.org/wiki/POODLE> for details.

When establishing SSL connection in Java, applications start from protocol negotiation (SSL, TLS, TLSv1, etc.). The POODLE SSL fix ensures that no instance of ESM or ArcSight Web will accept connections of SSLv3 type; the protocol should be one of TLS protocols. The corresponding changes were made to the ArcSight Console, which is one of the ESM clients. No additional changes are required for the ArcSight Console. To access ArcSight Command Center the web-browser should allow the use of TLSv1 protocols, which is the default setting for all web browsers.

## Usage Notes for this Patch

Also refer to ArcSight Express Release Notes Version 4.0. The usage notes for that release also apply to this patch.

## Upgrade to Latest Connector Versions

In order to receive POODLE attack protection for your connectors, be sure to upgrade to the latest version of each connector. The connector upgrades will provide the latest POODLE attack protection and JRE version. These upgrades need to be performed in addition to the installation of ArcSight Express 4.0 Patch 1, and are not part of the patch installation.

## Section 508 Compliance

ArcSight recognizes the importance of accessibility as a product initiative. To that end, ArcSight continues to make advances in the area of accessibility in its product lines.

## Geographical Information Update

This version of ArcSight Express includes an update to the geographical information used in graphic displays. The version is GeoIP-532\_20150101.

## Vulnerability Updates

This release includes recent vulnerability mappings from the January 2015 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 1232 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT
Enterasys Dragon IDS updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S840 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
Juniper / Netscreen IDP update 2458 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSKB, MSSB, CERT
McAfee Intrushield updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, CERT, MSSB
TippingPoint UnityOne DV8653 updated	Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, MSKB, CERT

Device	Vulnerability Updates
ISS SiteProtector updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB, MSKB, CERT
Symantec Endpoint Protection updated	Faultline, Bugtraq, CVE, X-Force, Nessus
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	Bugtraq

## Installing ArcSight Express 4.0 Patch 1

You can install this patch release using the platform-specific component executable files provided. Patch installers are available for all supported platforms. Keep the following points in mind when installing Patch 1:



- **For all components and platforms:** Make sure that you have enough space available *before* you install the patch. The installer checks for 3 GB of space and generates an error if it is not available. If you run into disk space issues during installation, create enough space, restore the component base build from the backup, then resume patch installation.
- Backup, patch install, and uninstall procedures require permissions for the relevant components. To install a patch, make sure that the user who owns the base build installation folder has full privileges on the PATH where the base build is installed.
- To uninstall the software you must be at the same user level as the original installer.
- It is a good practice to create a backup of the existing product before installation begins. 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.
- For backup, patch install, and uninstall, we recommend that you log in to the target machine with a specific account name via telnet or SSH. If you switch accounts after logging in, then specify the flag "-" for the **su** command (`su - <UserName>`).

Each component has install and uninstall steps.

## Verify AE 4.0 Patch 1 Files

HP provides a digital private key to enable you to verify that the signed software you received is indeed from HP and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

## ArcSight Express Main Component Suite

This section describes how to install or uninstall the ArcSight Express 4.0 Patch 1 for all the main components except the ArcSight Console. These components include the Manager, ArcSight Web, ArcSight Management Center, Connector Appliance, and the CORR-Engine.

### To Install the Patch



- Before you install the patch, verify that <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 Stop the ArcSight services as user *arcsight*.

```
/sbin/service arcsight_services stop all
```

- 2 Back up the ArcSight directory, `/opt/arcsight`, by making a copy. Place the copy in a readily accessible location. This is just 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 patch into `/home/arcsight` from the HP Software Support Online site (<http://softwaresupport.hp.com>):

```
ArcSightExpressSuitePatch-XXXX.tar
```

where XXXX represents the suite build number.

Ensure that the patch installer is downloaded into `/home/arcsight`. The installation will not launch properly if the installer is downloaded to any other location. Be sure to verify the patch file; see [“Verify AE 4.0 Patch 1 Files” on page 7](#).

- 4 Run the following command to extract the patch installer from the tar file as user *arcsight*:

```
tar -xvf ArcSightExpressSuitePatch-XXXX.tar
```

- 5 To install, run one of the following commands as user *arcsight* from the shell prompt and then follow the instructions presented on the shell.

To install in the GUI mode run:

```
./ArcsightExpressSuitePatch.bin
```

To install in the Console mode run:

```
./ArcsightExpressSuitePatch.bin -i console
```

- 6 Read through the license agreement and accept it at the end. In GUI mode, the acceptance radio button is disabled until you scroll to the bottom of the agreement. In the console mode, press **Enter** until you have paged through to the end of the license agreement.

- 7 Check the pre-installation summary for accuracy. Click **Install**.



- 8 Click **Next** on the File Delivery Complete screen to install the Manager, and ArcSight Web components.
- 9 Read carefully the instructions on the Install Complete screen and click **Done**.
- 10 Start the ArcSight services as user *arcsight*:

```
/sbin/service arcsight_services start all
```

**Note**

Check ArcSight services status and make sure that `mysqld` process is running before running the `tzupdater.sh` script in the next step:

```
/sbin/service arcsight_services status mysqld
```

- 11 Change directory as user *root* and update timezone data:

```
cd /home/arcsight/tzupdater/  
./tzupdater.sh
```

- 12 Run the following command as user *root*:

```
cp /opt/arcsight/services/init/arcsight-services-cleanall.conf  
/etc/init
```

Answer *y* when prompted whether to overwrite the file.

## To Uninstall the Patch

If needed, use the procedure below to roll back this patch installation and restore the system to the pre-patched state.

**Note**

Before you begin to uninstall, verify that the Manager's `<ARCSIGHT_HOME>` and any of its subdirectories are not being accessed by any open shells on your system.

- 1 Stop the ArcSight services as user *arcsight*.

```
/sbin/service arcsight_services stop all
```

**Note**

The uninstaller will prompt you to stop services if services are running.

- 2 Run the uninstaller program from either the directory where you created the link while installing the product or, if you had opted not to create a link, then run this from the `/opt/arcsight/UninstallerData_4.0.0.1` directory:

```
./Uninstall_ArcSightExpressSuitePatch
```

Alternatively, you can run the following command from the `/home/arcsight` (or wherever you installed the shortcut link) directory:

```
./Uninstall_ArcSightExpressSuitePatch
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSightExpressSuitePatch -i console
```

Run the uninstaller in the same mode (GUI or Console) in which you ran the installer.

- 3 Read carefully the instructions on the Uninstall Complete screen and click **Done**.
- 4 Navigate to `/opt/arcsight/services/init` and do the following:  
  

```
Rename arcsight-services-cleanall.conf.pre4.0.0.1 to  
arcsight-services-cleanall.conf  
  
mv arcsight-services-cleanall.conf.pre4.0.0.1  
arcsight-services-cleanall.conf  
  
Rename arcsight-monit.conf.pre4.0.0.1 to arcsight-monit.conf  
  
mv arcsight-monit.conf.pre4.0.0.1 arcsight-monit.conf
```
- 5 Restart services by running the following command as user *root* or as user *arcsight*:  
  

```
/sbin/service arcsight_services start all
```
- 6 Change directory as user *root* and rollback timezone data:  
  

```
cd /home/arcsight/tzupdater/  
./tzupdater.sh uninstall
```

**Note**

Check ArcSight services status and make sure that `mysqld` process is running before running the above script.

---

- 7 Run the following command as user *root*:  
  

```
cp /opt/arcsight/services/init/arcsight-services-cleanall.conf  
/etc/init
```

  
Answer `y` when prompted whether to overwrite the file.

## ArcSight Console

This section describes how to install or uninstall the ArcSight Express 4.0 Patch 1 for ArcSight Console on Windows, Mac, and Linux platforms.

**Tip**

The ArcSight ESM Console is not supported on AIX or Solaris. The following steps do not include information for installing a Console patch on those platforms.

---

## To Install the Patch

**Note**

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



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.

Download the executable file specific to your platform from the HP Software Support Online site (<http://softwaresupport.hp.com>). YYYY.Y represents the Console build number.

- ◆ Patch-6.1.0.YYYY.Y-Console-Win.exe
- ◆ Patch-6.1.0.YYYY.Y-Console-Linux.bin
- ◆ Patch-6.1.0.YYYY.Y-Console-MacOSX.zip

For the Mac, see [To Install the Patch on a Macintosh](#), below.

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

◆ **On Windows:**

Double-click Patch-6.1.0.YYYY.Y-Console-Win.exe

◆ **On Linux:**

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

```
./Patch-6.1.0.YYYY.Y-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-6.1.0.YYYY.Y-Console-Linux.bin -i console
```

The installer launches the Introduction window.

- 4 Read the instructions provided and click **Next**.
- 5 Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
- 6 Enter the location of your existing <ARCSIGHT\_HOME> directory for your 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 Link Location (on Linux) or Shortcut location (on 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 a Macintosh

The patch installer download and run procedure is slightly different on the Macintosh 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 just a precautionary measure so you can restore the original state, if necessary.
- 3 Download the file `Patch-6.1.0.YYYY.Y-Console-MacOSX.zip` to anywhere on your system.



The patch installer file shows as a **ZIP** file on the download site, but downloads as `ArcSightConsolePatch.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. There is no need to “extract” or “unzip” the file; it downloads as an **APP** file.

---

- 4 Launch the patch installer by double-clicking the `ArcSightConsolePatch` file.
- 5 Follow the steps on the patch install wizard, providing the information as prompted:
  - ◆ Accept the terms of the license agreement and click **Next**. The acceptance radio button is disabled until you scroll to the bottom of the agreement.
  - ◆ Choose the location where you want to install the patch. Browse to `<ARCSIGHT_HOME>`, where your previous Console was installed.
  - ◆ Choose an alias location for the Console application (or opt to not use aliases). This is the same as a link location on UNIX systems or shortcut location on Windows systems.
- 6 Click **Next**.
- 7 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>` 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:

**On 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 > All Programs > ArcSight Express Console 4.0 Patch 1 > Uninstall ArcSight Express Console 4.0 Patch 1**

- ◆ Or, run the following from the Console's  
<ARCSIGHT\_HOME>\current\UninstallerData\_6.1.0.1 directory:  
Uninstall\_ArcSight\_Console\_Patch

#### On Linux:

- ◆ From the directory where you created the link when installing the Console (your home directory or some other location), run:  
./Uninstall\_ArcSight\_Console\_4.0.0.1
- ◆ Or, to uninstall using Console mode, run:  
./Uninstall\_ArcSight\_Console\_4.0.0.1 -i console
- ◆ If you did not create a link, execute the command from the Console's  
<ARCSIGHT\_HOME>/current/UninstallerData6.1.0.1 directory:  
./Uninstall\_ArcSight\_Console\_Patch

#### On a Mac:

- ◆ From the directory where you created the link when installing the Console, run:  
Uninstall\_ArcSight\_Console\_4.0.0.1
- ◆ From the Console's  
<ARCSIGHT\_HOME>/current/UninstallerData\_6.1.0.1 directory, run:  
Uninstall\_ArcSight\_Console\_Patch

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

## Issues Fixed in this Patch

The following issues are fixed in this patch.

### Analytics

Issue	Description
NGS-8876	In a Query, the GetHour variable returned the hour translated from local time to GMT. For example, if your local time is 20:31:47, the GetHour variable might return 3, instead of 20, as expected. This is now fixed.
NGS-8875	The Day function now converts timestamp data correctly. For the event count history, the Event Count Last 7 Days query viewer now shows the correct data.

## ArcSight Console

Issue	Description
NGS-9520	<p>If a customer opened a Query Viewer, adjusted the column widths, and then clicked Refresh, the column widths would return to default size. We have improved this functionality so that the column widths remain as changed until the ArcSight Console session is closed. (When you log in again the defaults are restored.)</p> <p>Note that if you click Refresh repeatedly and rapidly enough, the Query Viewer columns will return to the default widths.</p>
NGS-9298	<p>Queries used in the report or query viewer or channel have a performance issue when there is a large amount of event annotation data. This fix resolves this issue by optimizing the query time dynamically. Enable the <code>event.annotation.optimization.enabled</code> property in the <code>server.properties</code> file. When this property is true, it uses the new optimization feature. Otherwise, it behaves as usual. You are only affected by this change if you need the optimization, in which case, set the property to true.</p> <p><b>Note:</b> This fix is certified in a stand-alone deployment only. Other limitations apply. Contact HP Technical Support with any concerns.</p>
NGS-8180	<p>When used in reports, the Get Hour function was yielding the wrong value. This is now fixed.</p>
NGS-3123	<p>Active channel loaded slowly when a request URL file name was used in the active channel filter.</p> <p>This issue is now fixed.</p>

## ArcSight Database

Issue	Description
NGS-8874	<p>The Instance of MySQL was getting into an inconsistent state during shutdown, which could lead to data corruption.</p> <p>Improvements have been made to the shutdown script to fix this issue.</p>
NGS-5063	<p>Under certain loads, an unstable condition could on occasion arise that leads to a Signal 11 occurrence. This patch provides a significant improvement to reduce the likelihood of a Signal 11 condition.</p>

## ArcSight Manager

Issue	Description
NGS-8301	<p>Event aggregation set for a number of matches within a time frame would also include matches outside that time frame,</p> <p>Now only matches within the specified time frame are aggregated.</p>

## Installation and Upgrade

Issue	Description
NGS-10616	<p>If you start the ArcSight Express 4.0 Patch1 CORRE installation wizard, then navigate back and forward using the Previous and Next buttons (for example, to reset configuration options on previous screens), but then exit from the wizard without actually installing, the base component fails to launch. The same launch failure occurs if you cancel the installation at any point. This is because the preparatory step of backing up the files has already occurred. If you encounter this situation, the workaround is to restore the functionality of the base Console by running the following commands to restore the backup files:</p> <p>On Linux:</p> <pre> Login as user arcsight cd /home/arcsight; mkdir /home/arcsight/rollback; cd /home/arcsight/rollback; unzip ../preinstall_rollback.zip; chmod +x install_rollback.sh; ./install_rollback.sh; Start the services: /sbin/service arcsight_services start </pre> <p>Please contact customer support for further details.</p>
NGS-10929	<p>This Patch release provides the POODLE SSL fix.</p> <p>The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit that takes advantage of Internet and security software clients' fallback to SSL 3.0. See <a href="http://en.wikipedia.org/wiki/POODLE">http://en.wikipedia.org/wiki/POODLE</a> for details.</p> <p>When establishing SSL connection in Java, applications start from protocol negotiation (SSL, TLS, TLSv1, etc.). The POODLE SSL fix ensures that no instance of ESM or ArcSight Web will accept connections of SSLv3 type; the protocol should be one of TLS protocols. The corresponding changes were made to the ArcSight Console, which is one of the ESM clients. No additional changes are required for the ArcSight Console. To access ArcSight Command Center the web-browser should allow the use of TLSv1 protocols, which is the default setting for all web browsers.</p>

## Open Issues in this Patch

This release contains the following open issues. Use the workarounds, where available.

## Installation and Upgrade

Issue	Description
NGS-11260	<p>In some instances, you might be unable to uninstall the ArcSight Express 4.0 Patch 1 console from your Mac OS workstations.</p> <p>In this case, to remove ArcSight Express 4.0 Patch 1, delete the current installation folder of ArcSight Express 4.0.</p>

Issue	Description
NGS-11760	Attempting to stop services by running <code>/sbin/services arcsight_services stop</code> as the user <code>arcsight</code> can result in a syntax error. Workaround: Run <code>/sbin/services arcsight_services stop</code> as the user <code>root</code> .
NGS-11761	Attempting to stop services by running <code>/sbin/service arcsight_services stop</code> when all services are already down causes the command to take over 10 minutes to terminate, and to then indicate it failed. Workaround: Run <code>/sbin/services arcsight_services status</code> to check status before running <code>/sbin/service arcsight_services stop</code> . If all services are already unavailable, there is no reason to run the <code>/sbin/service arcsight_services stop</code> command.

## Connectors

Issue	Description
NGS-11154	If the you are running out of the box connectors, then you must use the latest version certified with the POODLE fix.



## Open and Closed Issues in ArcSight Express 4.0

For information about open and closed issues for ArcSight Express 4.0 see the release notes for that version.

