

Release Notes

ArcSight ESM 6.0c Patch 1

February 28, 2013



Copyright © 2013 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>

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) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
02/28/2013	ESM 6.0c Patch 1	Release Notes for ESM 6.0c Patch 1 release

Contents

ArcSight ESM Version 6.0c Patch 1	5
ESM 6.0c Patch 1	5
Purpose of this Patch	5
Usage Notes for this Patch	5
Section 508 Compliance	5
Geographical Information Update	5
Vulnerability Updates	6
Installing ESM Version 6.0c Patch 1	6
ArcSight ESM Main Component Suite	7
ArcSight Console	8
Issues Fixed in this Patch	11
Analytics	11
ArcSight Console	11
ArcSight Manager	12
ArcSight Web	12
CORR-Engine	13
Open Issues in this Patch	13
ArcSight Console	13
ArcSight Manager	13
ArcSight Web	14
CORR-Engine	14
Open and Closed Issues in ESM 6.0c	14

ArcSight ESM Version 6.0c Patch 1

ESM 6.0c Patch 1

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

This patch is for ArcSight ESM 6.0c only. To set up a new ESM 6.0c installation, refer to the ArcSight ESM Installation and Configuration Guide.

After you have installed 6.0c, follow the instructions in [“Installing ESM Version 6.0c Patch 1” on page 6](#) of these release notes to apply Patch 1.

Purpose of this Patch

This patch:

- Addresses critical issues in ESM 6.0c
- Provides updates for geographical information and vulnerability mapping.

Usage Notes for this Patch

Refer to ArcSight™ ESM Release Notes Version 6.0c. The usage notes for that release also apply to this patch.

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 ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20120501.

Vulnerability Updates

This release includes recent vulnerability mappings (January 2013 Context Update) for these devices:

Device	Vulnerability Updates
Snort / Sourcefire SEU 777 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
Enterasys Dragon IDS updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
Cisco Secure IDS S687 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2222 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
TippingPoint UnityOne DV8405 updated	Faultline, Bugtraq, CVE, Nessus, MSSB
ISS SiteProtector updated	Faultline, Bugtraq, CVE, Nessus, X-Force, CERT, MSSB
Symantec Endpoint Protection updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSKB, MSSB, CERT
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	CVE

Installing ESM Version 6.0c Patch 1

You can install this patch release using the platform-specific and component-specific executable files provided. Patch installers are available for all supported platforms.

Please 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 begin to install the patch. The installer checks for 1 GB of space and will generate an error if that is not available. If you run into disk space issues during installation, first create enough disk space, restore the component base build from the backup, then resume installation of the patch.
- 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.
- It is a good practice to create a backup of the existing product before installation begins.
- To uninstall the software you must be at the same user level as the original installer.
- 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.

ArcSight ESM Main Component Suite

This section describes how to install or uninstall the ESM 6.0c Patch 1 for all the main components except the ArcSight Console. These components include the Manager, ArcSight Web, and the CORR-Engine.

To Install the Patch



Note

- 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 (for example, /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.



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 patch from the HP Software Support Online site (<http://support.openview.hp.com>).

```
ArcSightESMSuitePatch-1254.tar
```

- 4 Extract the tar file and run the patch installer as user *arcsight*:

```
./ArcSightESMSuitePatch.bin
```

- 5 Select the mode. For GUI mode, you must have the Linux GUI enabled. Otherwise, use the Console mode.
- 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 Select a location for the uninstaller link, if you want to have a shortcut to the uninstaller in some other location. You must have write permission to the specified folder.
- 8 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.
- 9 Click **Install**.
- 10 Click **Next** on the File Delivery Complete screen to install the CORR-Engine, Manager, and ArcSight Web components.
- 11 Click **Done** on the Install Complete screen.
- 12 Restart the ArcSight services as user *arcsight*:

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

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
```

- 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/suitepatch/UninstallerData_6.0.0.1 directory:

```
./Uninstall_ArcSight_ESM_Suite_Patch
```

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

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.0.0.1
```

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

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

ArcSight Console

This section describes how to install or uninstall the ESM 6.0c 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.

**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 executable file specific to your platform from the HP Software Support Online site (<http://support.openview.hp.com>).
 - ◆ Patch-6.0.0.1378.1-Console-Win.exe
 - ◆ Patch-6.0.0.1378.1-Console-Linux.bin
 - ◆ For the mac, see [To Install the Patch on a Mac](#), below.
- 4 Run one of the following executables specific to your platform:
 - ◆ **On Windows:**
Double-click Patch-6.0.0.1378.1-Console-Win.exe
 - ◆ **On Linux:**
Verify that you are logged in as user *arcsight*, and then run the following command:


```
./Patch-6.0.0.1378.1-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-6.0.0.1378.1-Console-Linux.bin -i console
```


The installer launches the Introduction window.
- 5 Read the instructions provided and click **Next**.
- 6 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.
- 7 Enter the location of your existing <ARCSIGHT_HOME> directory for your 6.0 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**.
- 8 Click **Next**.
- 9 Choose a Link Location (on Linux) or Shortcut location (on Windows) by clicking the appropriate radio button and click **Next**.
- 10 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.
- 11 Click **Install**.
- 12 Click **Done** on the Install Complete screen.

To Install the Patch on a 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 just a precautionary measure so you can restore the original state, if necessary.

- 3 Download the file `Patch-6.0.0.1378.1-Console-MacOSX.zip` to anywhere on your system.



The patch installer file (that shows as a **ZIP** file on the download site) 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 Console 6.0c Patch 1 > Uninstall ArcSight Console 6.0c Patch 1

- ◆ Or, run the following from the Console's `<ARCSIGHT_HOME>\current\UninstallerData_6.0.0.1` directory:
`Uninstall_ArcSight_ESM_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_ESM_Console_6.0.0.1
```

- ◆ Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Console_6.0.0.1 -i console
```

- ◆ If you did not create a link, execute the command from the Console's <ARCSIGHT_HOME>/current/UninstallerData6.0.0.1 directory:

```
./Uninstall_ArcSight_ESM_Console_Patch
```

On a Mac:

- ◆ From the directory where you created the link when installing the Console, run:

```
Uninstall_ArcSight_Console_6.0.0.1
```
- ◆ From the Console's <ARCSIGHT_HOME>/current/UninstallerData_6.0.0.1 directory, run:

```
Uninstall_ArcSight_ESM_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-3955	<p>The /All Active Lists/ArcSight Administration/ESM/System Health/Resources/Query Running Time was a partially-cached active list. At high EPS, it sometimes created a performance impact.</p> <p>The list has been changed from a partially-cached active list to a regular active list and the capacity is changed to 500k, so this issue no longer occurs.</p>
NGS-1999	<p>On a system with a high EPS scheduled rules may not fire. If you have a system, perhaps one with a high EPS, in which the scheduled rules are not running quickly enough, you can enable them to run in parallel (multi-threading) to speed them up. Add the following property to the server.properties file:</p> <pre>rules.replay.run.parallel=true</pre> <p>You can also set the number of threads to use, as follows (the default if you do not use this property is four threads):</p> <pre>rules.replay.numthreads=<number of threads to use></pre>

ArcSight Console

Issue	Description
NGS-4550	<p>Previously, when running a scheduled trend, the Console log sometimes showed the message "java.lang.ClassCastException: java.lang.Long cannot be cast to java.lang.Integer." This message should not have occurred.</p> <p>This is now fixed.</p>
NGS-4387	<p>Previously the HTML text in a payload viewer used non-HTML line breaks. These are now replaced with HTML line breaks:
.</p>
NGS-4056	<p>Previously, the payload value in ArcSight Web would be HTML encoded. without the fix, the payload value with html was rendered and an XSS vulnerability was encountered. This issue is now fixed.</p>

ArcSight Manager

Issue	Description
NGS-4335	Memory leak in CORR-E caused Manager to become unresponsive. This is now fixed.
NGS-4202	Channel would attempt to refresh event information when an initial query for event data timed out, rather than leaving row as "loading event." This issue is now fixed.
NGS-3775	When a user is enabled or disabled for login, an event with name "User updated" is generated. This event did not indicate whether login was enabled or disabled for this user. This is now fixed. The enabled/disabled information is now kept in "Device Custom String6". To use this information, you can, for example, add the column "Device Custom String6" to "System Events Last Hour" channel. This column will either say "enabled" or "disabled."
NGS-3771 TTP#52583	There is a new feature that automatically deactivates any user account that has been inactive for more than 90 days. After installing this patch run the "arcsight managersetup" command to implement this feature. Then restart the Manager. To change the inactive period add the property auth.user.account.age=<days> to the Manager's server.properties file, change <days> to the number of days you want, and restart the Manager.

ArcSight Web

Issue	Description
NGS-5004	Previously, the exception stack would display in the page source. This is now fixed by the addition of a new property. To NOT display the exception stack in page source, add the following property in webserver.properties: web.display.exception.stack=false Then clear the browser cache.
NGS-4219	A report would fail to run if a web user logged in to the ArcSight Web Console and selected a user's email address for 'Email to' option. The problem occurred when the web user was configured with an Active Directory external id. This issue is now fixed.
NGS-4124	Previously, the payload value in ArcSight Web would be HTML encoded. Without the fix, the payload value with HTML was rendered and an XSS vulnerability was encountered. This issue is now fixed.
NGS-3989	The ArcSight Web Login banner displayed newline characters as \n instead of adding a new line. Now this banner displays correctly.

CORR-Engine

Issue	Description
NGS-4893	In a disaster-recovery scenario where event archives were restored onto a brand new, plain vanilla system, you could not restore annotations for event archives that were in the online state. This fix resolves that problem. The offline archives were unaffected.
NGS-4229	Archive stopped working after Daylight Saving Time ended in Brazil at midnight on 10/22 when the clock was turned back one hour. The following error that appeared in the Logger log file: "An archive with duplicate date already exists in the database". This issue is now fixed.
NGS-3948	When restoring archives from an old ESM 6.0c system to another ESM 6.0c system, if the archives contained forwarded events, the restore of that archive would fail due to a highly restrictive eventID check. Now the restore properly accounts for forwarded events.
NGS-3921	Previously, the command "arcsight_services restart mysqld" did not properly restart the mysql process. This command now works correctly.

Open Issues in this Patch

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

ArcSight Console

Issue	Description
NGS-4091	Console hangs due to arc_notification_history and arc_notification_registry too big. You can solve the problem by editing the file /opt/arcsight/logger/data/mysql/my.cnf to set innodb_buffer_pool_size = 512M (the default was 128). Then restart all services.

ArcSight Manager

Issue	Description
NGS-3856	When you try to display an Active List with a large number of entries (for example 10 million entries), you get an error in the server.log file. Workaround: Increase the memory size for ESM to ensure that the Active List size is within limit. Also, if possible, avoid displaying Active Lists with a large number of records.

ArcSight Web

Issue	Description
NGS-3990	<p>Under some circumstances when you select the Knowledge Base link in ArcSight Web, navigating the user interface fails to work correctly.</p> <p>The workaround is to log out, clear the browser cache and log back in.</p>

CORR-Engine

Issue	Description
NGS-4082	<p>If the buffer pool is too small, it can cause slow channel performance or prevent logging in to the Console. If you get an error message like this:</p> <pre>[ERROR][default.com.arcsight.common.persist.mysql.MysqlNotificationBroker][purgeOldNotifications]</pre> <p>java.sql.SQLException: The total number of locks exceeds the lock table size</p> <p>You can solve the problem by editing the file /opt/arcsight/logger/data/mysql/my.cnf to set innodb_buffer_pool_size = 512M (the default was 128).</p> <p>Then restart all services.</p>

Open and Closed Issues in ESM 6.0c

For information about open and closed issues for ESM 6.0c see the release notes for that version.