Release Notes
ArcSight ESM

Version 6.5c Patch 1

March 10, 2014

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI.
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
3/10/2014	ArcSight ESM Version 6.5c Patch 1	Release Notes for ArcSight ESM Version 6.5c Patch 1

Contents

ArcSight ESM Version 6.5c Patch 1

ESM 6.5c 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 6.5c only. To set up a new ESM 6.5c installation, refer to the ArcSight ESM Installation and Configuration Guide.
The build number for the ESM suite for this patch is 1736
The build number for the ArcSight Console for this patch is 1837.1.

After you have installed 6.5c, follow the instructions in "Installing ESM Version 6.5c Patch 1" on page 6 of these release notes to apply Patch 1.

Purpose of this Patch

This patch:

- Addresses critical issues in ESM 6.5c.
- Provides updates for geographical information and vulnerability mapping.

Usage Notes for this Patch

Refer to ArcSight ESM Release Notes Version 6.5c. 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_20140201.

Vulnerability Updates

This release includes recent vulnerability mappings from the February 2014 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU-1052 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT, MSSB
Enterasys Dragon IDS updated	Faultline, CVE, Nessus, MSSB
Cisco Secure IDS S771 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2344 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB, CERT
TippingPoint UnityOne DV8524 updated	Faultline, Bugtraq, CVE, Nessus, MSSB
ISS SiteProtector updated	Bugtraq, CVE, X-Force, CERT
Symantec Endpoint Protection updated	Bugtraq, CVE
McAfee HIPS 7.0 updated	CVE
Radware DefensePro updated	CVE

Installing ESM Version 6.5c Patch 1

You can install this patch release using the platform-specific component 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 install the patch. The installer checks for 1 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.

ArcSight ESM Main Component Suite

This section describes how to install or uninstall the ESM 6.5c 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

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

   ```
   ArcSightESMSuitePatch-XXXX.tar
   ```

   ...where `XXXX` represents the suite build number.

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

   ```
   ./ArcSightESMSuitePatch.bin
   ```

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

   ```
   ./ArcSightESMSuitePatch.bin -i console
   ```

5. 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.

6. 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.

7. 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.

8. Click **Install**.

9. Click **Next** on the File Delivery Complete screen to install the CORR-Engine, Manager, and ArcSight Web components.

10. Click **Done** on the Install Complete screen.

11 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.

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_6.5.0.1` 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_6.5.0.1
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.5.0.1 -i console
```

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

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

4 Restart services by running the following command as user *root* or as user *arcsight*:

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

ArcSight Console

This section describes how to install or uninstall the ESM 6.5c Patch 1 for ArcSight Console on Windows, Mac, and Linux platforms.

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

- 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.

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.

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

- `Patch-6.5.0.YYYY.Y-Console-Win.exe`
- `Patch-6.5.0.YYYY.Y-Console-Linux.bin`
- `Patch-6.5.0.YYYY.Y-Console-MacOSX.zip`

For the Mac, see To Install the Patch on a Mac, below.

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

   - **On Windows**:

     Double-click `Patch-6.5.0.YYYY.Y-Console-Win.exe`

   - **On Linux**:

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

     ```
     ./Patch-6.5.0.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-6.5.0.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 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-6.5.0.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 ESM Console 6.5c Patch 1 > Uninstall ArcSight ESM Console 6.5c Patch 1

- Or, run the following from the Console's `<ARCSIGHT_HOME>\current\UninstallerData_6.5.0.1` 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_6.5.0.1`

- Or, to uninstall using Console mode, run:

  `./Uninstall_ArcSight_ESM_Console_6.5.0.1 -i console`

- If you did not create a link, execute the command from the Console's `<ARCSIGHT_HOME>/current/UninstallerData6.5.0.1` 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_6.5.0.1`

- From the Console's `<ARCSIGHT_HOME>/current/UninstallerData_6.5.0.1` 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.

CORR_Engine

Issue	Description
NGS-8252	Under certain loads, an unstable condition could on occasion arise that leads to a Signal 11 occurrence. This patch release provides a significant improvement to reduce the likelihood of a signal 11 condition.

Analytics

Issue	Description
NGS-8251	Under some circumstances, events had incorrect severity values. This is now fixed.

Open Issues in this Patch

This release contains no new open issues.

Open and Closed Issues in ESM 6.5c

For information about open and closed issues for ESM 6.5c, see the release notes for that version.