Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 6.9.1c Patch 1

Release Notes

March 31, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

ArcSight ESM 6.9.1c 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 fixed and open issues.

This patch is for ArcSight ESM 6.9.1c only. To set up a new ESM 6.9.1c installation, refer to the ArcSight ESM Installation and Configuration Guide.
The build number for the ESM suite for this patch is 2075.
The build number for the ArcSight Console for this patch is 2250.1

After you have installed 6.9.1c , follow the instructions in "Installing ESM Version 6.9.1c Patch 1" on page 6 of these release notes to apply Patch 1.

Purpose of this Patch

This patch:

- Updates the JRE to 1.7.0_97
- Enable HA environment on newly certified OS versions in this Patch.
- Addresses critical issues in ESM 6.9.1c.
- Provides updates for geographical information and vulnerability mapping.
- Provides important security updates.

Refer to the HPE ArcSight ESM Support Matrix for the new and existing operating systems supported in this patch.

Usage Notes

SSL Client Authentication After Patch Installation

If you have configured SSL Client Authentication prior to applying this patch, and if you used keytoolgui to generate keypairs and certificates, then you must re-generate them after applying the patch and before re-starting services.

Enable Iframe of Command Center Pages

To allow iframing of Command Center pages, you can add the following optional setting in server.properties:

```
allow.from.domains=entries
```

Where entries are a comma separated list of the elements that could be of one of the following two forms:

- origin (for example, `https://hpe.com`)
- `key:::origin`

In this example, the key is any string uniquely identifying the origin within the comma-separated list. For the definition of origins, see http://tools.ietf.org/html/rfc6454.

Below is an example of "allow.from.domains" containing several entries. The first entry is origin, while the second is key-value pair:

```
allow.from.domains=https://hpe.com,microsoft:::https://microsoft.com
```

Third party applications that need to iframe Command Center pages should add the parameter "origin" to URLs pointing to Command Center page and use that parameter to specify their origin. For example:

```
https://host:8443/www/ui-
phoenix/com.arcsight.phoenix.PhoenixLauncher/?origin=microsoft#login
```

In that parameter the origin could be specified directly (https://microsoft.com) or with help of the key (microsoft) from the above ESM configuration setting.

ESM uses "origin" parameter from HTTP request to lookup an entry in "allow.from.domains" setting. If there is matching entry, then iframing is allowed for configured origin. If origin is specified in the HTTP request, but is not presented in "allow.from.domains", the request will fail with the exception "Not allowed request".

HTTP requests without "origin" parameter are handled by ESM the same way as before, so there are no changes for regular Command Center sessions. Here iframing is not allowed to prevent clickjacking vulnerability:

```
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
```

The implementation requires enabling cookies in the browser. It might also be needed to login to Command Center without iframing from the browser once. Opening Command Center directly creates browser's cookie for the target host. By default, the cookies for iframed pages are not created.

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_2016601.

Vulnerability Updates

This release includes recent vulnerability mappings from the May 2016 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 1495 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
Cisco Secure IDS S925 updated	Faultline, Bugtraq, CVE, Nessus
Juniper / Netscreen IDP update 2738 updated	Faultline, Bugtraq, CVE, Nessus, MSSB
McAfee Network Security Manager 8.7.79.3 updated	Faultline, CVE, Nessus, MSSB
TippingPoint UnityOne DV8831 updated	MSSB
IBM Security Host Protection for Desktops 3260 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 36.060 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3260 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 36.060 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 36.060 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Server IPS for Linux technology 36.060 updated	Faultline, CVE, Nessus, X-Force
IBM RealSecure Server Sensor XPU 36.060 updated	Faultline, CVE, Nessus, X-Force
McAfee Host Intrusion Prevention 7.0/8.0 content version 7007	CVE

Installing ESM Version 6.9.1c Patch 1

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

Note: 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 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.

Verifying the Downloaded Installation Software

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

Visit the following site for information and instructions:

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

ArcSight ESM Main Component Suite

This section describes how to install or uninstall the ESM 6.9.1c Patch 1 for all the main components except the ArcSight Console. These components include the Manager and the CORR-Engine.

To Install the Patch

Note: Installation considerations:

- 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.

- HPE recommends that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

1. Download the patch from the HPE Software Support Online site (http://softwaresupport.hpe.com).

   ```
   ArcSightESMSuitePatch-XXXX.tar
   ```

   ...where XXXX represents the suite build number.

   Be sure to verify the patch file; see "Verifying the Downloaded Installation Software" on the previous page.

2. As user *arcsight*, extract the `tar` file.
3. Stop the ArcSight services as user *arcsight*:

   ```
   /etc/init.d/arcsight_services stop all
   ```

4. Back up the ArcSight directory, `/opt/arcsight`, by making a copy. Place the copy in a readily accessible location. This is a precautionary measure so you can restore the system to the original state, if necessary.

   Caution: HPE 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.

5. If you have High Availability configured, run the following command on the secondary server as user *root* to put the server in standby mode:

   crm_standby -v true

6. From the directory where you extracted the tar file, 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
   ```

7. 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 console mode, press the **Enter** key until you have paged through to the end of the license agreement.
8. 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.
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. Press **Enter** to start the installation.
11. When the installation is complete press **Enter** to Exit.

> **Note:** If you have configured SSL Client Authentication prior to applying this patch, and if you used keytoolgui to generate keypairs and certificates, then you must re-generate them after finishing applying the patch and before re-starting services.

12. Start the ArcSight services as user *arcsight*:

    ```
    /etc/init.d/arcsight_services start all
    ```

13. If you have High Availability configured, run the following command on the secondary server as user *root* to bring the server online:

    ```
    crm_standby -D
    ```

To Uninstall the Patch

If needed, use the procedure below to uninstall 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*:

   ```
   /etc/init.d/arcsight_services stop all
   ```

2. If you have High Availability configured, run the following command on the secondary server as user *root* to put the server in standby mode:

   ```
   crm_standby -v true
   ```

3. As user *arcsight*, 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_6.9.1.1/UninstallerData_6.9.1.1` 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_6.9.1.1
   ```

   Or, to uninstall using Console mode, run:

   ```
   ./Uninstall_ArcSight_ESM_Suite_Patch_6.9.1.1 -i console
   ```

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

4. When the installation is complete press **Enter** to Exit.
5. Start the ArcSight services as user *arcsight*:

   ```
   /etc/init.d/arcsight_services start all
   ```

6. If you have High Availability configured, run the following command on the secondary server as user *root* to bring the server online:

   ```
   crm_standby -D
   ```

ArcSight Console

This section describes how to install or uninstall the ESM 6.9.1c 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:** Installation considerations:
>
> - 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.
> - HPE recommends that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

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:** HPE 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 HPE Software Support Online site (http://softwaresupport.hpe.com). `YYYY.Y` represents the Console build number.
   - `Patch-6.9.1.YYYY.Y-Console-Win.exe`
   - `Patch-6.9.1.YYYY.Y-Console-Linux.bin`
   - `Patch-6.9.1.YYYY.Y-Console-MacOSX.zip`

     Be sure to verify the patch file; see "Verifying the Downloaded Installation Software" on page 7.

     For the Mac, see "To Install the Patch on a Mac" on the next page.

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

- **On Windows**:
  Double-click `Patch-6.9.1.YYYY.Y-Console-Win.exe`
- **On Linux**:

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

  ```
  ./Patch-6.9.1.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-6.9.1.YYYY.Y-Console-Linux.bin -i console
  ```

  The installer launches the Introduction window.

5. Read the instructions provided and Press **Enter**.
6. Accept the terms of the license agreement and press **Enter**. In GUI mode the acceptance radio button is disabled until you scroll to the bottom of the agreement. In Console mode, press **Enter** until you have read every page, and then Press **Enter** to accept the agreement.
7. Select the location of your existing `<ARCSIGHT_HOME>` directory for your Console installation by typing the appropriate choice and pressing **Enter**

   If you want to restore the installer-provided default location, select **Restore Default Folder**.
8. Press **Enter** to continue.
9. Select a Link Location (on Linux) or Shortcut location (on Windows) by clicking the appropriate radio button and Press **Enter** or 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. Press **Enter** to start the installation.
12. When the installation is complete, press **Enter** to exit..

    Note: If you have configured SSL Client Authentication prior to applying this patch, and if you used keytoolgui to generate keypairs and certificates, then you must re-generate them after finishing applying the patch and before re-starting services.

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.

Note: HPE recommends that you continue through the installation and do not attempt to cancel the installation process or move backward through the installer windows.

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-6.9.1.YYYY.Y-Console-MacOSX.zip` to anywhere on your system.

   > **Tip:** 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.

   Be sure to verify the patch file; see "Verifying the Downloaded Installation Software" on page 7.

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 uninstall 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.
>
> If you setup SSL Client Authentication or PKCS11 tokens for authentication after this patch was applied, then before you uninstall it, make a backup of the JRE's cacerts file on the Console machine. The file path (using Windows as an example) is Console\current\jre\lib\security\cacerts. After uninstall is finished, overwrite the JRE's cacerts file with the backup you made. Otherwise, authentication may fail.

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 6.9.1c Patch 1 > Uninstall ArcSight ESM Console 6.9.1c Patch 1

- Or, run the following from the Console’s `<ARCSIGHT_HOME>\current\UninstallerData_6.9.1.1` directory:

  ```
  Uninstall_ArcSight_ESM_Console_Patch.exe
  ```

- On Windows 8.1, run the following from the Console's `<ARCSIGHT_HOME>\current\UninstallerData_6.9.1.1` directory:

  ```
  Uninstall_ArcSight_ESM_Console_Patch.exe
  ```

  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_Patch_6.9.1.1
  ```

- Or, to uninstall using Console mode, run:

  ```
  ./Uninstall_ArcSight_ESM_Console_Patch_6.9.1.1 -i console
  ```

- If you did not create a link, execute the command from the Console’s `<ARCSIGHT_HOME>/current/UninstallerData_6.9.1.1` directory:

  ```
  ./Uninstall_ArcSight_ESM_Console_Patch
  ```

- Or, to uninstall using Console mode, run:

  ```
  ./Uninstall_ArcSight_ESM_Console_Patch -i console
  ```

  On a Mac:

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

  ```
  Uninstall_ArcSight_ESM_Console_Patch_6.9.1.1
  ```

- From the Console’s `<ARCSIGHT_HOME>/current/UninstallerData_6.9.1.1` directory, run:

  ```
  Uninstall_ArcSight_ESM_Console_Patch
  ```

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

   > **Note:** If you are on a Windows system and you plan to uninstall the base build Console after uninstalling Patch 1, be advised that your system restarts without warning upon finishing the base build uninstallation. Prepare your system accordingly.

Fixed Issues

The following issues are fixed in this release.

ArcSight Console

Issue	Description
NGS-18270	Event ID column was not visible to the ArcSight Console interface. The visibility of the Event ID column has been enabled. This issue is now fixed.
NGS-18269	When adding columns using the Customize Columns feature in an active channel, the added columns would appear blank, or missing data. This issue is now fixed.
NGS-13393	Connector's Filter tab is now viewable by users with read-only permissions.
NGS-13390	Previously the "Last Password Change" date/time value would change to the time of the last login, and passwords never expired. Now, even after restarting the ArcSight Console The "Last Password Change" remains as the date/time when the password was actually changed.
NGS-11782	The following pop up dialogs will remain on the same screen with console on windows. Inline Filter - Condition Editor pop-up dialog Tools - Configure, Results, Nslookup, Ping, PortInfo, Traceroute, and Whois pop-up dialogs

ArcSight Manager

Issue	Description
NGS-18065	For an active list that defines the Date type field in its key or defines the Date type field without specifying a key, the value in its count field was sometimes not updated correctly. This issue is now fixed.
NGS-18064	During active list import from a CSV file and under certain conditions, date fields would be imported as NULL. This issue is now fixed.

Issue	Description
NGS-17738	In order to turn on debug logging, set all "level value" to "DEBUG" in file <ARCSIGHT_HOME>/manager/arcsight-dm/plugins/com.arcsight.dm.plugins.logging_1.0.0/logConfiguration.xml Then restart the Manager for this change to take effect.
NGS-16701	Users can now adjust the maximum attachment size up to 100 MB for reports that are sent as email attachment, by setting the report.upload.maxFileSize property to the desired size (in MB) in the server.properties file. Refer to the ESM Admin Guide to learn how to change the ESM configuration using property files.
NGS-13873	Previously, when importing a package (default) with an active list, the "Last Modified Time" on the active list was changed to when the package was imported. Thus, the original "Last Modified Time" is not preserved, which could cause issues with syncing TTL for active list entries across two systems. Now, a property has been added to the defaults.server.properties file to keep the Last Modified Time unchanged for entries in an active list imported from a package: entry.lastmodifiedtime.enabled=true

CORR-Engine

Issue	Description
NGS-17810	When running an SQL query via 'arcdt' or using an ESM resource that produces an SQL query (for example, Active Channel, Query/Query Viewer, or Report), and the conditions of the SQL query contained some IP address constants, either via 'IN()', or multiple = predicates, combined by 'OR' operators, the SQL query could produce incorrect results. This issue has been fixed.

Connector Management

Issue	Description
NGS-13888	Previously, after going through the connector import wizard, the configuration changes appeared for the connector resource in the ArcSight Console, when viewed in the Inspect/Edit window. However, running agentsetup did not show that the changes had taken effect. Now, the Import Connector Configuration feature, correctly updates the connector as well.

Open Issues

This release contains the following open issues.

Command Center

Issue	Description
NGS-20048	When using Internet Explorer 11 with ActivClient middleware and a PKCS#11 token, an error is displayed stating 'This page can't be displayed', preventing the user from logging to ArcSight Command Center. if there are problems with PIN dialog to log in to the card in some client (Firefox, IE, Chrome, ArcSight Console), try another client. Once the card is successfully authenticated through that client, the middleware (e.g. ActivClient) might skip card authentication, when you repeat PKCS#11 login from the original client.

Installation and Upgrade

Issue	Description
NGS-19860	When uninstalling the Console Patch on Mac, if the actual uninstaller binary located in <CONSOLE_HOME>/current/UninstallerData_6.9.1.1 is used to invoke the uninstall process, then the UninstallerData_6.9.1.1 directory is left behind after the process finishes. Workaround: Use the symbolic link created when the Patch was installed to invoke the Console Patch Uninstaller on Mac, instead of the binary directly. Or delete the ArcSight Console's UninstallerData_6.9.1.1 directory, you can now re-install ArcSight Console ESM patch.

Open and Closed Issues in ESM 6.9.1c

For information about open and closed issues for ESM 6.9.1c, see the release notes for that version.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (ESM 6.9.1c Patch 1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!