



Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 6.9.1c Patch 2

Release Notes

November 21, 2016

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

© Copyright 2016 Hewlett Packard Enterprise Development, LP

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 2	4
Purpose of this Patch	4
Usage Notes	5
SSL Client Authentication After Patch Installation	5
Enable iframe of Command Center Pages	5
Nested Storage Groups	6
Preserving Reference Pages Information	6
Authentication Between IE 11 and PKCS#1 Token	6
Corrections to the High Availability Module User's Guide	6
Uninstalling the Console Patch on the Mac	7
Section 508 Compliance	8
Geographical Information Update	8
Vulnerability Updates	8
Installing ESM Version 6.9.1c Patch 2	9
Verifying the Downloaded Installation Software	9
ArcSight ESM Main Component Suite	9
To Install the Patch	10
To Uninstall the Patch	11
ArcSight Console	12
To Install the Patch	12
To Install the Patch on a Mac	14
To Uninstall the Patch	14
Fixed Issues	16
Analytics	16
ArcSight Console	16
ArcSight Manager	17
CORR-Engine	17
Command Center	17
General	18
Open Issues	20
Open and Closed Issues in ESM 6.9.1c Patch 1	20
Send Documentation Feedback	21

ArcSight ESM 6.9.1c Patch 2

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, with or without a released patch. 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 2120.

The build number for the ArcSight Console for this patch is 2310.

After you have installed 6.9.1c with or without a released patch, follow the instructions in ["Installing ESM Version 6.9.1c Patch 2" on page 9](#) of these release notes to apply Patch 2.

Purpose of this Patch

This patch:

- Updates the JRE to 1.7.0_101
- Supports RHEL 6.8 and CentOS 6.8 for those upgrading from ESM 6.8c to ESM 6.9.1c Patch 2
- Enables High Availability (HA) environment on newly certified OS versions of RHEL 6.8 and CentOS 6.8 for upgraded ESM 6.8c to 6.9.1 Patch 2.

Note: If you are on ESM 6.8 Patch 4 with HA configuration on RHEL or CentOS 6.8 and you are planning to upgrade to ESM 6.9.1 and subsequent patches, refer to the document, *Upgrade from ESM 6.8 Patch 4 to ESM 6.9.1c on RHEL/CentOS 6.8: Technical Note*. Download this document from [Protect 724](#).

- 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 regenerate them after applying the patch and before restarting 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.

Nested Storage Groups

When creating a storage group in the ArcSight Command Center, do not nest this new group under an existing group: this means the archiving path of one group must not be under the archiving path of another group. Nesting storage groups increases the archive space utilization for that group.

For information about storage and archiving, refer to the *ArcSight Command Center User's Guide*.

Preserving Reference Pages Information

This information applies to tiered ESM architectures where the network model would be similar across ESM installations, and would therefore have the same networks and zones. When you are forwarding events from a source to a destination in this type of architecture, the Reference Pages information (a resource group attribute) would be the same in the source and in the destination.

If the Reference Pages information for a given resource group is not found in the destination, make sure the Network attribute of the forwarding connector is set. Then make sure the specified network belongs to a zone. It is important that your network model is defined correctly, and that connector configurations have the correct Network setting. This connector setting applies to all connectors being used, including Forwarding Connector.

Authentication Between IE 11 and PKCS#1 Token

When using Internet Explorer 11 with ActivClient middleware and a PKCS#11 token, an error is displayed:

This page can't be displayed

This prevents the user from logging into ArcSight Command Center.

if there are problems with the PIN dialog to log into the card in some client (Firefox, IE, Chrome, ArcSight Console), try another client. Once the card is successfully authenticated through that client, the middleware (for example ActivClient) might skip card authentication, when you repeat PKCS#11 login from the original client.

Corrections to the High Availability Module User's Guide

Corrections are needed on pages 20 and 21 of the *ESM High Availability Module User's Guide for ESM 6.9.1*. The topic applies to ESM Appliance used in high availability configurations.

Page with error	Description
20	<p>Step c directs you to edit the <code>.bash_profile</code> script in the root user's home directory.</p> <p>Correction:</p> <p>This step needs to add that you must perform this on both appliances, the primary and secondary.</p>
21	<p>The first bullet on this page provides commands to run on both appliances if you are converting a single-installation appliance to an HA Module cluster installation.</p> <p>Correction:</p> <p>The bullet and commands should be replaced with:</p> <p>Run the following commands as root on both the primary and the secondary appliance:</p> <pre>systemctl stop hp-asrd hp-health hp-snmp-agents mv /opt/hp /usr/local ln -s /usr/local/hp /opt umount /opt ln -s /usr/local/hp /opt mount /opt systemctl start hp-asrd hp-health hp-snmp-agents</pre>
21	<p>The third to the last paragraph states:</p> <p>"If the systems in the cluster are two appliances (ESM Express or ESM Appliance), then skip this step. The metadata partition already exists on each system."</p> <p>Correction:</p> <p>This paragraph should state</p> <p>If the systems in the cluster are two appliances, then the metadata partition already exists, and is named</p> <pre>/dev/sda6</pre>

Uninstalling the Console Patch on the Mac

When uninstalling the Console Patch on the Mac, if the actual uninstaller binary located in `<CONSOLE_HOME>/current/UninstallerData_6.9.1.2` is used to invoke the uninstall process, then the `UninstallerData_6.9.1.2` 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 the Mac, instead of the binary directly. Or delete the ArcSight Console's `UninstallerData_6.9.1.2` directory. After deleting, you can re-install the ArcSight Console ESM 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_20160901.

Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire 2983 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
Enterasys Dragon IDS updated	CVE
Cisco Secure IDS S941 updated	Bugtraq, CVE
Juniper IDP update S941 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
TippingPoint UnityOne DV8868 updated	Faultline, MSSB
IBM Security Host Protection for Desktops 3320 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 36.090 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3320 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 36.090 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 36.090 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Server IPS for Linux technology 36.090 updated	Faultline, CVE, Nessus, X-Force
IBM RealSecure Server Sensor XPU 36.090 updated	Faultline, CVE, Nessus, X-Force
McAfee HIPS 7.0 updated	CVE

Installing ESM Version 6.9.1c Patch 2

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 2:

- **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.

Caution: Do not interrupt the patch install process (for example, do not press Ctrl-C or log off). Interrupting the process would cause issues.

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 2 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_6.9.1.2/UninstallerData_6.9.1.2` 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_6.9.1.2
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.9.1.2 -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 2 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 9.

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 9](#).

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 2 > Uninstall ArcSight ESM Console 6.9.1c Patch 2

- Or, run the following from the Console's <ARCSIGHT_HOME>\current\UninstallerData_6.9.1.2 directory:

`Uninstall_ArcSight_ESM_Console_Patch.exe`

- On Windows 8.1, run the following from the Console's <ARCSIGHT_HOME>\current\UninstallerData_6.9.1.2 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_6.9.1.2`

- Or, to uninstall using Console mode, run:

`./Uninstall_ArcSight_ESM_Console_Patch_6.9.1.2 -i console`

- If you did not create a link, execute the command from the Console's <ARCSIGHT_HOME>/current/UninstallerData_6.9.1.2 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_6.9.1.2`

- From the Console's <ARCSIGHT_HOME>/current/UninstallerData_6.9.1.2 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 2, 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.

• Analytics	16
• ArcSight Console	16
• ArcSight Manager	17
• CORR-Engine	17
• Command Center	17
• General	18

Analytics

Issue	Description
NGS-19751	Warnings could occur in the log file indicating that "Trend query took too much time," even if the query was finished before the timeout limit. This issue has been fixed.
NGS-14897	Rules that were disabled by the Rules Engine are now re-enabled automatically on startup.

ArcSight Console

Issue	Description
NGS-19745	The ESM query editor did not maintain the "distinct" parameter when the "order by" section was edited. This issue has been fixed.
NGS-19222	In order to restrict the maximum number of active channels opened by a user, the property server.channel.maxchannels needs to be set in the server.properties configuration file. Note: changing the property in the console.properties file has no effect. Also note: increasing this parameter leads to a strong possibility of performance degradation, so caution is advised.

ArcSight Manager

Issue	Description
NGS-20144	The informational message "Skipped mac-address mis-match check" was logged as an error. It is now logged at the appropriate level.
NGS-13299	Creation and last updated timestamps, and user IDs, were not preserved when case resources were imported. Now if the parameter "case.infonote.enabled" is set to "true" in the server.properties file, a note containing the original Creation Time, Last Modified Time, creator ID and modifier ID will be created for each case imported. Note: this will only be possible with packages created in 6.9.1 Patch 2 or later.
NGS-11138	Active Channel with cases was not properly refreshed if it was opened in two consoles by the same user, data was refreshed only in one console. Now data in active channel are refreshed for all consoles with any user.

CORR-Engine

Issue	Description
NGS-20319	When calculating space utilization, storage groups whose archive path was under another storage group archive path were counted twice This issue has been fixed.

Command Center

Issue	Description
NGS-19961	New private Fieldset type was added to ArcSight Command Center. Private Fieldset can be used and edited only by author.

General

Issue	Description
NGS-21192	MRT field in the arc_event_annotation was not in sync with event's MRT when events were annotated. The issue is now fixed.
NGS-20938	The following conditions did not always work as filter conditions for an active channel: Event Annotation Stage Name != "Closed" Event Annotation Stage Name != "Incident" The issue is now fixed.
NGS-20147	It was observed that the case channels were displaying duplication of case data. The bug fix ensures that the duplicate cases do not appear in case channels. The case channels now show one instance of a case that matches a filter as against multiple instances of same case.
NGS-20143	Using a query with custom parameters which are enumerations within a report resulted in empty output reports being generated. This has been fixed.
NGS-20085	Annotation information failed to be set correctly when the event was marked as isReviewed. The issue is now fixed.
NGS-19747	Events with timestamps outside a particular range can be adjusted to Manager receipt time or dropped. Use the following settings (with defaults) in the server.properties file to enable this capability: event.time.corrector.enabled (false) event.time.corrector.dropbad (false) event.max.negative.time.offset (default/minimum -1 day) event.max.positive.time.offset (default/minimum +1 day) If the corrector is enabled and event timestamps are within the configured range, no action is taken. If the corrector is enabled and events with timestamps outside the configured range are received, the specified action is taken for those events only, and audit messages are generated. If needed, standard rules can be configured to send notifications when such audit messages are received.
NGS-19746	When a user was moved to another group and a link was created, and after that selected for deletion, if you did not confirm the deletion in the popup screen and closed the window, the user was deleted anyway. Now, if you close the delete confirmation popup without confirming, the deletion is cancelled.
NGS-19744	An ambiguous error would occur in the logs where there was a problem with the type of a dependent variable. The error message has been augmented to include more specific information about the error.
NGS-19579	After upgrade from ESM6.8c to ESM6.9.1, notifications could result in an error "[base URL not configured, run managersetup]". Running managersetup would not resolve the problem. This condition has been fixed.

Issue	Description
NGS-19493	ESM ran out of JVM memory in few cases. The issue is now fixed.
NGS-19475	If the MySQL database password for user 'arcsight' contains a space character, the command /opt/arcsight/manager/bin/arcsight export_system_tables will not be able to connect to the database, and fail. This issue has been fixed for passwords with internal spaces. Passwords with leading and trailing spaces are not supported.
NGS-19267	It was not possible to restrict access to cases by user in ACC. A new property has been created to allow this. In order to enable the functionality, set "restrict.access.to.cases" to "true" in the server.properties file, then use "Edit Access Control" in ArcSight Console. Existing cases will not be affected.
NGS-19235	When new entries are added to a specific active lists, some of the records (random behavior) can't be deleted. The issue is now fixed.
NGS-18852	Before ESM6.8, when using the ArcSight admin console to Import and Export Connector Configurations, a user could choose to "Select All" or individually check the box in the "Override" column for the configuration items to import. This functionality has been restored.
NGS-18247	If an Active List had more than 20 columns of type "String" and a user attempted to Apply Settings, ESM would indicate a MySQL syntax error. This issue has been fixed.
NGS-17417	With more than 500 correlated events attached to a case editing the case will take a long time under load. The issue is now fixed.
NGS-9813	Behind the scenes manager creates a report in order to export all events from the active channel. Therefore the report must have a report template and a specified filter or filters. In order the user to be able to export all events in the active channel, user must have the following permissions: Read access to /All Report Templates/ArcSight System/1 Table/ Read access to the specified event's filter. For example: If a user belongs to a User Group which has in the Edit Access Control Panel , in the Events tab , read access to /All Filters/ArcSight System/Events Types/ArcSight Correlation Events then the user must have read access to /All Filters/ArcSight System/Events Types/ in the Resources tab as well.

Open Issues

The following issue is open in this release.

Issue	Description
NGS-17417	With more than 500 correlated events attached to a case editing the case will take a long time under load.

Open and Closed Issues in ESM 6.9.1c Patch 1

For information about open and closed issues for ESM 6.9.1c Patch 1, see the release notes for that release.

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 2)

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!