



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight ESM**

Software Version: 6.8c Patch 4

## Release Notes

September 29, 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

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

# Contents

ESM 6.8c Patch 4 .....	5
Purpose of this Patch .....	5
Usage Notes for this Patch .....	5
Documentation Errata .....	6
Topic “Setting up SSL Client Authentication on ArcSight Web” Omitted from ESM 6.8c Administrator’s Guide .....	6
ESM High Availability Module User’s Guide 1.0 - Improvements to Change Hostname or IP Address Topics .....	6
Improve Display of Russian Language PDF Reports .....	6
Localized Environment - How to Configure Time and Date Display in Report Tables .....	7
Setting Up to Use ActivClient’s Common Access Card (CAC) .....	7
ArcSight Web Configuration for PKCS#11/CAC .....	8
Enable Iframe of ArcSight Command Center Pages .....	8
Upgrading from ESM 6.8 Patch 4 on RHEL 6.8 or CentOS 6.8 to ESM 6.9.1c .....	9
Section 508 Compliance .....	9
Geographical Information Update .....	10
Vulnerability Updates .....	10
Installing ESM Version 6.8c Patch 4 .....	10
Verify ESM 6.8c Patch 4 Files .....	11
ArcSight ESM Main Component Suite .....	11
To Install the Patch .....	11
To Uninstall the Patch .....	13
ArcSight Console .....	14
To Install the Patch .....	14
To Install the Patch on a Mac .....	15
To Uninstall the Patch .....	16
Fixed Issues .....	17
Analytics .....	18
ArcSight Console .....	18
ArcSight Manager .....	19
CORR-Engine .....	20
Command Center .....	20
Open Issues .....	20
ArcSight Console .....	21

Installation and Upgrade .....	21
Command Center .....	21
Issues Fixed in Previous Patches .....	21
Analytics .....	22
ArcSight Console .....	22
ArcSight Manager .....	24
ArcSight Web .....	25
CORR-Engine .....	26
Command Center .....	26
Installation and Upgrade .....	27
Open and Closed Issues in ESM 6.8c .....	27
 Appendix A: Omitted Text for Section “Setting Up SSL Client Authentication on ArcSight Web” ..	28
Setting Up SSL Client Authentication on ArcSight Web .....	28
 Send Documentation Feedback .....	34

# ESM 6.8c Patch 4

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 fixed issues.

This patch is for ArcSight ESM 6.8c only, with or without released patches. To set up a new ESM 6.8c installation, refer to the ArcSight ESM Installation and Configuration Guide.

The build number for the ESM suite for this patch is 2095.

The build number for the ArcSight Console for this patch is 2285.4.

After you have installed 6.8c (with or without released patches), follow the instructions in "[Installing ESM Version 6.8c Patch 4](#)" on page 10 of these release notes to apply Patch 4.

## Purpose of this Patch

This patch:

- Updates the JRE to 1.7.0\_101
- Enables you to download HA Upgrade Files from the HPE Software Support Online site (<http://softwaresupport.hpe.com>) if you are working in an ESM 6.8c HA environment. Follow the upgrade HA environment guide to upgrade the environment.
- Addresses critical issues in ESM 6.8c; applicable to ESM 6.8c with or without ESM 6.8c patches.
- Provides updates for geographical information and vulnerability mapping.
- Provides important security updates.
- Provides numerous Japanese language translation improvements

Refer to the [HPE ArcSight ESM Support Matrix](#) for the new and existing operating systems supported in this patch.

## Usage Notes for this Patch

Refer to ArcSight ESM Release Notes for version 6.8c, including those for Patches 1, 2, and 3 if needed.

The usage notes for those previous releases also apply to this patch.

## Documentation Errata

### Topic “Setting up SSL Client Authentication on ArcSight Web” Omitted from ESM 6.8c Administrator’s Guide

Refer to ["Setting Up SSL Client Authentication on ArcSight Web" on page 28](#) for this text.

### ESM High Availability Module User's Guide 1.0 - Improvements to Change Hostname or IP Address Topics

The following topics in the ESM High Availability Module User's Guide 1.0 have been improved to include more detailed commands on changing server hostnames or IP addresses:

- Changing the Secondary Hostname or IP Address Only
- Changing the Primary Hostname or IP Address Only
- Changing Both Server Hostnames or IPs

This updated guide is available on Protect 724 at <https://www.protect724.hpe.com/docs/DOC-11931>. Download it to get the latest version of this information.

## Improve Display of Russian Language PDF Reports

PDF reports in Russian language can display with no spaces between words. This problem occurs because some Cyrillic language fonts that are TrueType fonts are not supported directly by versions of Adobe Reader earlier than version 8.0. In order to work around this, each TrueType font must be mapped to an OpenType font supported in Adobe Reader 8.0. ArcSight provides this mapping in the `<ARCSIGHT_HOME>/i18n/server/reportpdf_config_<locale>.properties` file. You have the option to change the default mapping of any TrueType font to the OpenType font by modifying the respective font mapping in this file.

To work around this issue, HPE recommends that you:

1. Install a localized Adobe Reader 8.0 depending on the language of your platform on your Manager machine. This version of the Adobe Reader installs the OpenType fonts by default.
2. Edit the `server.properties` file as follows:
  - a. Set `report.font.trueType.path` property to point to the directory that contains the TrueType and OpenType font. Use ":" as a path separator in Unix. On Unix platforms, the TrueType font path may differ depending on the specific Unix platform, but it is typically `/usr/lib/font`. The CIDFont directory is always the same relative to the Adobe Reader installed directory. So, the default directory would be `/usr/lib/font:<adobe_reader_dir>/Resource/CIDFont`.

- b. Set `report.font.cmap.path` property to point to Adobe Reader's CMap directory. On Unix, the CMap path is relative to the Adobe Reader installation -- `<adobe_reader_dir>/Resource/CMap`.

## Localized Environment - How to Configure Time and Date Display in Report Tables

This issue applies only to ESM deployed in a localized environment. The changes suggested below affect the report parameters only, not the report data.

Modify the following parameters in `server.properties` to configure the date format and display the correct time and date in your reports:

```
# The date format for all report content
```

```
report.content.dateFormat=dd MM yyyy HH:mm:ss
```

```
# The date format for datetime report parameters (e.g. $CurrentDateTime, $Now)
```

```
report.datetime.dateFormat=dd-MM-yyyy-HH:mm:ss
```

```
# The date format for date report parameters (e.g. $CurrentDate)
report.date.dateFormat=dd-MM-yyyy
```

```
# The date format for month type report parameters (e.g. $CurrentMonth)
report.month.dateFormat=MM-yyyy
```

```
# The date format for week type report parameters (e.g. $CurrentWeek)
report.week.dateFormat=ww-yyyy
```

For details on editing the `server.properties` file, see the "Editing Properties Files" topic in the ESM Administrator's Guide.

## Setting Up to Use ActivClient's Common Access Card (CAC)

The steps to configure the CAC with ActivClient are added below. See Appendix C in the ESM 6.8c Installation and Configuration Guide for details.

1. Install the CAC Provider's Software on each client machine. That includes the ArcSight Console and every machine using a browser to access ArcSight Web or the Command Center

2. Map a User's External ID to the CAC's Subject CN.
3. Obtain the CAC's Issuers' Certificate.
4. Extract the Root CA Certificate From the CAC Certificate.
5. Import the CAC Root CA Certificate into the ArcSight Manager.
6. Import the CAC Root CA Certificate into the ArcSight Web.
7. Select Authentication Option in ArcSight Manager Setup or ACC Administration tab.
8. Select Authentication Option in ArcSight Web Setup.
9. Select Authentication Option in ArcSight Console Setup.

## ArcSight Web Configuration for PKCS#11/CAC

These steps to configure PKCS#11/CAC for the ArcSight Web are not in the Installation Guide.

### To configure:

1. Import the CAC card's root CA certificate into Web's <ARCSIGHT\_HOME>\config\jetty\webtruststore directory.
2. Set ArcSight Web's authentication to **Password Based or SSL Client Based Authentication** through webserversetup.

For further details, see the ESM Administrator's Guide.

**Note:** The authentication option for all the ESM components (ArcSight Manager, Console, and Web), should be matched with the selection of 'Password or SSL Client Based Authentication'. The respective component needs to be restarted after the change.

## Enable Iframe of ArcSight 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 a configured by administrator 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.

## Upgrading from ESM 6.8 Patch 4 on RHEL 6.8 or CentOS 6.8 to ESM 6.9.1c

If, after installing ESM 6.8c Patch 4, you upgrade your operating system to RHEL 6.8 or CentOS 6.8, and then want to further upgrade to ESM 6.9.1c, you must run this command as user *arcsight*:

```
mv /opt/arcsight/manager/config/upgrade/esm.supported.os.properties ~arcsight
```

If you do not run this command, and have performed the operating system upgrade and then try to upgrade from ESM 6.8c Patch 4 to ESM 6.9.1c, you will receive an error message stating that the operating system is unsupported.

## 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\_20160801.

## Vulnerability Updates

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

Device	Vulnerability Updates
Snort / Sourcefire SEU 1524 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
Enterasys Dragon IDS 20160810 updated	CVE
Cisco Secure IDS S934 updated	Faultline, Bugtraq, CVE, Nessus
Juniper IDP update 2771 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
McAfee Intrushield updated	Faultline, CVE, Nessus, MSSB
TippingPoint UnityOne DV8863 updated	Faultline, MSSB
IBM Security Host Protection for Desktops 3300 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Unix) 36.085 updated	Faultline, CVE, Nessus, X-Force
IBM Security Host Protection for Servers (Windows) 3300 updated	Faultline, CVE, Nessus, X-Force
IBM Proventia Network IPS XPU 36.085 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Network MFS XPU 36.085 updated	Faultline, Bugtraq, CVE, Nessus, X-Force, MSSB
IBM Proventia Server IPS for Linux technology 36.085 updated	Faultline, CVE, Nessus, X-Force
IBM RealSecure Server Sensor XPU 36.085 updated	Faultline, CVE, Nessus, X-Force
McAfee HIPS 7.0 updated	CVE

## Installing ESM Version 6.8c Patch 4

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 4:

- **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.

## Verify ESM 6.8c Patch 4 Files

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 6.8c Patch 4 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:** 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 "[Verify ESM 6.8c Patch 4 Files](#)" on the previous page.

2. As user *arcsight*, extract the tar file.
3. As user *root*, run the following command to stop and remove services:

```
sh /opt/arcsight/manager/bin/remove_services.sh
```

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 are using the High Availability Module, run the following command on the secondary server as user *root* to put the server in standby mode:

```
crm_standby -v true
```

6. 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 the console mode, press **Enter** 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. Click **Install**.
11. Click **Done** on the Install Complete screen.
12. As *root*, run *setup\_services* with this command:

```
sh /opt/arcsight/manager/bin/setup_services.sh
```

13. Check the ArcSight services as user *arcsight*:

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

14. If you are using the High Availability Module, run the following command on the secondary server as user *root* to bring the server on line:

```
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. As user *root*, run `remove_services` with this command:  

```
sh /opt/arcsight/manager/bin/remove_services.sh
```
2. If you are using the High Availability Module, 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_6.8.0.4/UninstallerData_6.8.0.4` 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_6.8.0.4
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.8.0.4 -i console
```

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

4. Click **Done** on the Uninstall Complete screen.
5. As *root*, run `setup_services` with this command:  

```
sh /opt/arcsight/manager/bin/setup_services.sh
```
6. If you are using the High Availability Module, run the following command on the secondary server as user *root* to bring the server on line:

```
crm_standby -D
```

## ArcSight Console

This section describes how to install or uninstall the ESM 6.8c Patch 4 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-6.8.0.YYYY.Y-Console-Win.exe
- Patch-6.8.0.YYYY.Y-Console-Linux.bin
- Patch-6.8.0.YYYY.Y-Console-MacOSX.zip

Be sure to verify the patch file; see "[Verify ESM 6.8c Patch 4 Files](#)" on page 11

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-6.8.0.YYYY.Y-Console-Win.exe

- **On Linux:**

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

```
./Patch-6.8.0.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-6.8.0.YYYY.Y-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 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.

**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-6.8.0.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 ["Verify ESM 6.8c Patch 4 Files" on page 11](#).

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:

- 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, back up the JRE's cacerts file on the Console machine. In Windows, for example, the path 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 6.8c Patch 4 > Uninstall ArcSight ESM Console 6.8c Patch 4**

- Or, run the following from the Console's <ARCSIGHT\_HOME>\current\UninstallerData\_6.8.0.4 directory:

Uninstall\_ArcSight\_ESM\_Console\_Patch

- On Windows 8, run the following from the Console's <ARCSIGHT\_HOME>\current\UninstallerData\_6.8.0.4 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_6.8.0.4
```

- Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Console_Patch_6.8.0.4 -i console
```

- If you did not create a link, execute the command from the Console's <ARCSIGHT\_HOME>/current/UninstallerData\_6.8.0.4 directory:

```
./Uninstall_ArcSight_ESM_Console_Patch
```

**On a Mac:**

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

```
Uninstall_ArcSight_ESM_Console_Patch_6.8.0.4
```

- From the Console's <ARCSIGHT\_HOME>/current/UninstallerData\_6.8.0.4 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 4, 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 .....	18
• ArcSight Console .....	18
• ArcSight Manager .....	19
• CORR-Engine .....	20
• Command Center .....	20

## Analytics

Issue	Description
NGS-11738	An audit event is generated whenever a report is sent to a recipient. Details pertaining to the status and content of the report, as well as details regarding the recipients, can be viewed with the "Custom Strings" section of the audit event.
NGS-14786	When ESM runs with a large number of active lists, long running reports, and trends, the ESM manager would run out of memory after a few days. This issue is now fixed.
NGS-14964	When an Active List had an error, the log message did not have enough detail to help you determine what the error was. These log messages now include the Event ID, Device Vendor, Field Name, and the schema type.
NGS-16595	Previously, pre-persistence rules were getting fired/invoked when they should not have been. Now only the events that satisfy the rule condition fire pre-persistence rules.
NGS-18038	When Active Lists were reimported from CSV files, some date fields would be empty. This issue has been fixed.
NGS-18039	When Active Lists were reimported from CSV files, some count fields would not be populated correctly. This issue has been fixed.
NGS-18595	After selected events with values in the "Raw Event" field were exported, the values were unexpectedly truncated. This issue is now fixed.
NGS-18742	Warnings could occur in the log file that "Trend query took too much time," even if the query was finished before the timeout limit.  This issue has been fixed.

## ArcSight Console

Issue	Description
NGS-9255	The size of files attached to cases can now be limited by the server, by adding the persist.file.size.max property to the config/server.properties file, and setting the value of this property to the desired maximum size in MB.
NGS-13085	The ESM query editor did not maintain the "distinct" parameter when the "order by" section was edited. This issue has now been fixed.
NGS-14461	When generating Excel reports, the graphs used a Java default number format, ignoring the report's template number format.  Now the report's template number format can be used instead of the current Java default number format, by setting the property by setting 'report.chart.value_label.use_template_value_format' to 'true' in the server.properties file.

Issue	Description
NGS-14855	<p>When an archived report is copied from one folder to another folder, then either is deleted, both the original and the copy of the report are deleted.</p> <p>This issue is now fixed.</p>
NGS-15072	<p>When a report is generated that is empty or too big, or failed to send, an audit event is now created in ESM to track the event.</p>
NGS-15682	<p>Searching on Notifications would return no results, because a search for Notifications resources has not been implemented for performance reasons. Therefore searching on that type of resource is disabled.</p> <p>To avoid confusion the dropdown menu for the resource search no longer contains the menu item for Notification</p>
NGS-16111	<p>When increasing the font size to 20px and 25px on the Console, the row height did not auto-resize on the active channel. Row height is now set according to the font size in grid view.</p>
NGS-16582	<p>Previously a SQL query would produce incorrect results under these circumstances:</p> <ul style="list-style-type: none"><li>- Running the query via 'arcdt' or</li><li>- Using an ESM resource that produces a SQL query (for example, Active Channel, Query/Query Viewer, or Report)</li><li>- The conditions of the SQL query contain some IP address constants</li><li>- The constants were either by way of 'INO', or multiple = predicates, and combined by 'OR' operators.</li></ul> <p>This issue has been fixed.</p>
NGS-17389	<p>Popup menu shows up on wrong monitor when screen extended vertically. The issue is now fixed. After you extend the monitors vertically then you must restart console in order the changes to take place.</p>
NGS-17581	<p>Case channels were displaying multiple rows of case data, one for each event attached to a case.</p> <p>Now duplicate cases do not appear in case channels</p>

## ArcSight Manager

Issue	Description
NGS-14338	<p>The informational message "Skipped mac-address mis-match check" was logged as an error. It is now logged at the appropriate level.</p>
NGS-14586	<p>In a disaster recovery situation, ambiguous errors would occur if the source and destination machines were set to different timezones. Now, if a timezone mismatch is detected, a useful error message is issued and the operation is aborted.</p>

Issue	Description
NGS-14927	<p>If you ran an empty report, you would get an email notification with the report's resource ID in the subject line, and in the message of the email. It was difficult to determine which report was being referenced.</p> <p>The issue is now fixed. When an email notification is sent regarding an empty report, the name of the report is displayed in the subject and in the message.</p>
NGS-17969	<p>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:</p> <p>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)</p> <p>If the corrector is enabled and events with timestamps are within the configured range, no action is taken.</p> <p>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.</p>

## CORR-Engine

Issue	Description
NGS-15465	<p>Previously, if you moved a user to another group, created a link, and later, selected that user for deletion, the user would be deleted even if you did not confirm the deletion.</p> <p>Now, if you close the deletion- confirmation popup window without confirming the deletion, the deletion action is canceled.</p>

## Command Center

Issue	Description
NGS-16206	<p>In the ArcSight Command Center, timestamps for stacked bar charts were ordered alphabetically rather than chronologically..</p> <p>This issue has been fixed</p>
NGS-19510	<p>AgentReceiptTime values were showing as epoch timestamps when events were exported from ArcSight Command Center to a CSV file.</p> <p>This issue has been fixed.</p>

## Open Issues

This release contains the following open issues.

- [ArcSight Console](#) .....21
- [Installation and Upgrade](#) .....21
- [Command Center](#) .....21

## ArcSight Console

Issue	Description
NGS-14853	On Windows, when uninstalling the base build after Patch 4 has already been uninstalled, after you ran the uninstaller program and clicked Done, the system restarted automatically with no prompt to let you choose whether to restart the system or not.

## Installation and Upgrade

Issue	Description
NGS-18134	<p>After uninstall, the empty folder UninstallerData_6.8.0.4 persists, if you uninstall the Console patch on Mac 10.9 by running the binary Uninstaller. This issues does not occur if you uninstall the patch using the Uninstaller link.</p> <p>Workaround:</p> <p>Manually remove the folder UninstallerData_6.8.0.4 in order to be able to reinstall the patch.</p>

## Command Center

Issue	Description
NGS-19560	<p>When adding peers, if you see an error message that says "PKIX path building failed", you need to manually configure the httpd.conf file by following these steps:</p> <ol style="list-style-type: none"><li>1. Open file /opt/arcsight/logger/current/local/apache/conf/httpd.conf and search for ServerName arcsight:9000</li><li>2. Change "arcsight" to the host's fully qualified domain name (FQDN) and save the file.</li><li>3. Restart Apache server by running:</li></ol> <pre>/etc/init.d/arcsight_services restart logger_httpd</pre>

## Issues Fixed in Previous Patches

The following issues are fixed in previous patches.

## Analytics

Issue	Description
NGS-14737	<p>Filters that were part of a Data Monitor could be moved by an admin to a location that user did not have access to. This caused the filter to become blank and the user was unable to change the filter.</p> <p>Now if an admin user moves a filter to a directory with a stricter ACL, an appropriate warning is presented, with an option to cancel.</p>
NGS-14581	<p>When attempting to create an Investigate Channel on a GV field in an active channel, there would be no result if the user did not have read permission on session lists.</p> <p>This issue is now fixed.</p>
NGS-14566	<p>When a Query was constructed with a GROUP condition using 'Sum', SQL generation would fail.</p>
NGS-11107	<p>Mapping certain Session List Global Variables (composed of multiple fields of different types) to a field with SetEventField action failed with errors.</p>
NGS-10996	<p>"Export to External System" action on a rule did not work properly.</p>
NGS-9757	<p>When a report included the "End Time" field, the time shown in that column was in the manager time zone instead of adjusted to the report query timezone.</p>
NGS-9505	<p>If a rule contains an action to AddToActiveList, and the action (or the enclosing trigger) is disabled, exporting the rule to the package will not include the referenced ActiveList, because the dependency relationship is not stored correctly. Consequently, importing the package on another system (either manually or automatically via Content Sync) may result in the rule being marked invalid.</p>

## ArcSight Console

Issue	Description
NGS-17451	<p>"Password Or SSLClient" was incorrectly translated in Japanese localization. This issue is now fixed.</p>
NGS-16076	<p>Monitor Events were not included in the replayfilegen utility, resulting in a number of events that was inconsistent with the Active Channel.</p> <p>This issue is now fixed.</p>
NGS-14933	<p>"Bucket size in seconds" was not translated correctly into Japanese.</p>
NGS-14791	<p>Translations of "Required package For" and "Optional package For" were not correct for Japanese.</p>
NGS-14723	<p>In some cases, event-based Active Channels that include an InCase filtering condition do not display events that belong to a case but have been removed from the main event table (arc_event) due to the retention period limit. Case-related events are copied to a special table so they can remain available after being archived, but the channel is unable to find and display such events correctly after the partition is archived.</p> <p>Workaround: Use the case event editor or Reports, which can correctly find and display these events.</p>

Issue	Description
NGS-14721	The "Moving Average" field in the Console Dashboard was translated incorrectly in Japanese.
NGS-14636	When many scheduled reports were running at the same time, an EPS drop could occur.  This issue is now fixed.
NGS-14584	Entries in active lists were considered identical with and without trailing spaces, and deletion of either would result in deletion of both entries.  This issue is now fixed.
NGS-14565	When case management was moved from ArcSight Web to ACC, the URL sent in email notifications was not updated correctly and still pointed to Web.
NGS-14525	Some archived reports that have Japanese characters in their names had garbled file names when downloaded, and the Japanese characters appeared blank.
NGS-14522	The Console displayed some incorrect Japanese translations. <ul style="list-style-type: none"> <li>• Login Console</li> <li>• Bucket size in Seconds</li> <li>• Number of Buckets</li> </ul> Also, the following are not translated into Japanese: <ul style="list-style-type: none"> <li>• The filtering being performed on the data monitor.</li> <li>• Bucket size in Seconds</li> <li>• Number of Buckets</li> <li>• Time Filed</li> <li>• The field to use for values</li> <li>• The file to aggregate data on</li> </ul>
NGS-14503	When using dual monitors (multiple display), filter operators would sometimes display on the wrong monitor. This issue is now fixed.
NGS-14483	Added support for a Static Banner at the top of every Console user interface connecting to a given Manager.  To do this, set the <code>server.staticbanner.backgroundcolor</code> , <code>server.staticbanner.textcolor</code> and <code>server.staticbanner.text</code> properties in <code>server.properties</code> and restart the Manager. The background color and textcolor properties only support the following color strings: black, blue, cyan, gray, green, magenta, orange, pink, red, white, yellow.  If the <code>server.staticbanner.text</code> is not set or empty then banner panel will not display. If the <code>server.staticbanner.backgroundcolor</code> is invalid or is not set then default color green will be used. If the <code>server.staticbanner.textcolor</code> is invalid or is not set then the default color black will be used.
NGS-14289	Filters applied to Connectors would show the filter conditions, rather than the Filter URI.  This issue is now fixed.
NGS-14160	When exporting from a non-empty active channel, a report could be created with zero events, due to mishandling of whitespace in the XML format.  This issue is now fixed.

Issue	Description
NGS-14113	<p>When manually overriding the status in a Last State Data Monitor, some were not visible if large images were used. This has been addressed by adding a scroll bar to the selection window.</p> <p>This issue is now fixed.</p>
NGS-13673	<p>When multiple recipients were provided in a scheduled report Jobs tab, for example: one user in Email To and one email address in Email Addresses; or two comma-separated email addresses in Email Addresses, then only the first email address in Email Addresses would receive the message.</p> <p>This issue is now fixed.</p>
NGS-12868	<p>When using ArcSight Command Center to export a report to CSV format, if the field set contained agentReceiptTime, the value was always blank because the export mechanism expected the database field name instead of the display name.</p>
NGS-12752	<p>When hotkeys were created for Profile Resources they did not work as expected.</p>
NGS-11515	<p>Data Monitors did not remember column field positions after being saved.</p>
NGS-10765	<p>Event ID column was not visible to the console interface. The visibility of Event ID column has been enabled.</p> <p>This issue is now fixed.</p>
NGS-7445	<p>When adding columns using the Customize Columns feature in an active channel, the added columns would appear blank, or missing data.</p> <p>This issue is now fixed.</p>

## ArcSight Manager

Issue	Description
NGS-16418	<p>A potential performance issue was discovered in ESM's resource handling. A data structure used in several places, including the Rules Engine, was unnecessarily exclusive-read locking, preventing multiple threads from accessing it simultaneously.</p> <p>Now, this potential performance issue is addressed by allowing concurrent reads in that data structure.</p>
NGS-14582	<p>When a rule tried to create a case using a filename as part of the case URI or case name, and that filename contained one or more embedded slashes (/ as in /etc/password), the embedded slashes were conflicting with internal representation causing the filename to be parsed into components. To prevent this misinterpretation, embedded slashes are now replaced with backslashes.</p> <p>This issue is now fixed.</p>
NGS-14567	<p>The value size calculations for integer/long/double values were incorrect, which could result in errors saying "Event ... is too long for DB column size '19'." in server.log.</p>
NGS-14130	<p>A new function, RoundN, is introduced in ESM 6.8c Patch 3. You can round a chosen field or variable containing a double number to between 0 and 5 decimal places.</p>
NGS-14056	<p>When a note was added to a resource, a "Note inserted" event was generated but was missing resource information. To address this, the missing information has been added to an audit event.</p>



Issue	Description
NGS-13222	Shutting down services by using the arcsight_services command might result in exceptions in the log file. These exceptions are due to an issue with the order in which the components are shut down, and can be safely ignored.
NGS-13146	Shutting down services by using the arcsight_services command might result in exceptions in the log file. These exceptions are due to an issue with the order in which the components are shut down, and can be safely ignored.
NGS-12491	Importing XML cases archive format files from the archive/imports directory was not working.  This issue is now fixed.
NGS-12341	By default, Instruments are not included in the Resource Validation Report. Customers now have to option to include them by adding the parameter includeTypes.  For example:  /opt/arcsight/manager/bin/arcsight resvalidate -includeTypes Instrument  Note: Resources are case sensitive, therefore inputting "instrument" will not work.
NGS-12225	Importing a CSV file into an active list with entries with the characters \n, \b, \t, \r (for example, C:\users\requests) causes the characters to appear erroneously in the ESM active list entry (e.g. C:\users\requests shows up as C:\usersequests). Also, when this data is exported into a csv file, the data displays erroneously (\n causes a newline space in the csv data).
NGS-11274	When using two consoles, in some conditions if the case information was edited in Console A, it was not replicated to Console B.
NGS-11273	When using two consoles, in some conditions if the case information was edited in Console A, it was replicated to Console B immediately, but it was not replicated to Console A when the case was edited in Console B.
NGS-11257	Prior to this fix, the password was not updated if it does not match the policy enforced (minimum length, previous password, etc.). The script would also silently fail meaning no error messages were displayed so the user would not know that the password was not updated.
NGS-10678	When pre-persistence rule sets "eventAnnotationStage" field value to any stages, this will cause flow exceptions and large numbers of events silently dropped. If the rule fires often, all events are dropped.

## ArcSight Web

Issue	Description
NGS-13261	Certain debug messages appear in logs. These messages have been turned off by default and can be turned on by editing  net.sf.j2ep.ProxyFilter.level=FINE in  /opt/arcsight/manager/arcsight-dm/logging.properties

## CORR-Engine

Issue	Description
NGS-17406	<p>The message "Logger server version is incompatible (should be 6.8.0.xxxx but is 6.8.0.yyyy)" was displayed in logger_web logs.</p> <p>The issue is now fixed.</p>
NGS-15922	<p>Full text search (the ability to search on any word of any text field of an event) is enabled by default. The disk space needed for storing events with full text search disabled should be approximately 40-50% of what is required with full text search enabled.</p> <p>To disable it, add the following line to the server.properties file and restart the ESM manager:</p> <p>fulltext.search.enabled=false</p>
NGS-14248	<p>Filters using Target and Attacker User Name fields were not working as expected in active channels or reports when used with ignore case.</p>
NGS-13403	<p>Case sensitive and insensitive queries sometimes returned wrong results when stored procedures or functions that return strings were used. Hence Active channels, Query Viewers and Reports gave wrong output when filtering events with and without the Ignore Case option.</p> <p>Note that there is a limitation to this fix in Russian locale as the version of MySQL used in the product has limitations with Cyrillic characters.</p>
NGS-11262	<p>Accessing instances of the THD class, part of an internal structure, intermittently caused a Signal 11 crash.</p>

## Command Center

Issue	Description
NGS-16779	<p>Some horizontal bar charts and moving average charts were not displayed correctly in ACC.</p> <p>This issue is now fixed.</p>
NGS-16771	<p>In the ArcSight Command Center while viewing Dashboard in Dashboard--&gt;Navigator page, for Last N events data monitor, Event ID data is shown in the Priority column and priority column appears misaligned.</p> <p>This issue is now fixed.</p>
NGS-14722	<p>Some archive reports with PDF format that have been ran and saved through ArcSight Command Center couldn't be opened, and this error displays:</p> <p>Cannot Run Report. Possible reason it might be invalid or No access to Report Template or Query.</p>
NGS-14525	<p>Some archived reports that have Japanese characters in their names have garbled file names when downloaded, and the Japanese characters are shown as blank.</p>

Issue	Description
NGS-14490	In an MSSP context, exporting search results using "Save to ArcSight Command Center" violates the separation between tenants within the system. To mitigate this by disabling the functionality, set <code>search.export.saveToServer.enabled=false</code> in <code>logger.properties</code> (as it is true by default/if absent).
NGS-14234	ArcSight Command Center (ACC) did not allow fields within cases (including those within the events panel) to be copied and pasted into external handling tools.  This issue is now fixed.
NGS-14169	When excluding Events in Search using alt-click, Fields with null were also not included.  A logger configuration " <code>sqlgenerator.querystr.addnullcondition</code> " can be added to enable the inclusion of the null value entries. The default value is false.
NGS-13631	When a query involving "OR" was used on the ArcSight Command Center in a multi-tenant environment, customer-specific filtering failed.
NGS-13037	ArcSight Command Center results are now presented with a shaded background on alternating rows.

## Installation and Upgrade

Issue	Description
NGS-12870	On the Windows platform, after uninstalling ArcSight ESM Console patch 6.8.0.2, the <code>UninstallerData_6.8.0.2</code> directory remains in the <code>&lt;Console/current&gt;</code> directory. This folder prevents ArcSight Console ESM patch 2 from installing again.  This issue is now fixed.
NGS-11761	Issuing a ' <code>arcsight_services stop</code> ' command when all services are down resulted in a failure 10 minutes later.
NGS-9142	Under certain circumstances, <code>arcsight_services</code> would report inconsistent status alternating between "available" and "unavailable".

## Open and Closed Issues in ESM 6.8c

For information about open and closed issues for ESM 6.8c, see the release notes for that version.

# Appendix A: Omitted Text for Section “Setting Up SSL Client Authentication on ArcSight Web”

This text was omitted from the ESM 6.8c Administrator’s Guide. It belongs after the topic “Setting Up SSL Client-Side Authentication on ArcSight Console” and before the topic “Setting Up Client-Side Authentication on SmartConnectors” in that guide.

## Setting Up SSL Client Authentication on ArcSight Web

To enable client-side authentication for clients running in default mode, perform these steps in addition to the ones you perform for setting up server authentication:

1. Generate a key pair on ArcSight Web. For CA-signed certificate follow the steps in section “Create a Key Pair for a CA-Signed Certificate” topic in the ESM Administrator’s Guide.
  - a. From the Web’s <ARCSIGHT\_HOME>/bin directory start keytoolgui by running the following command:

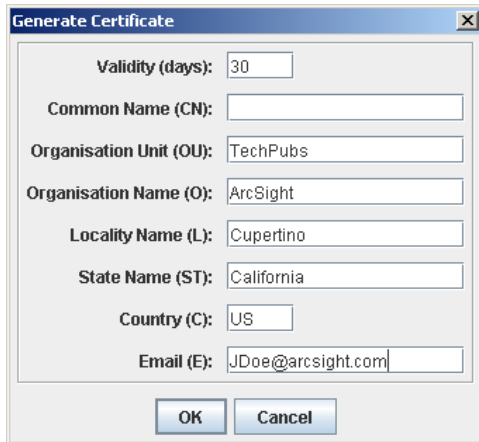
```
./arcsight keytoolgui
```

- b. Open **File->New keystore**. This opens the New keystore Type dialog.
  - c. Select **JKS** and click **OK**.

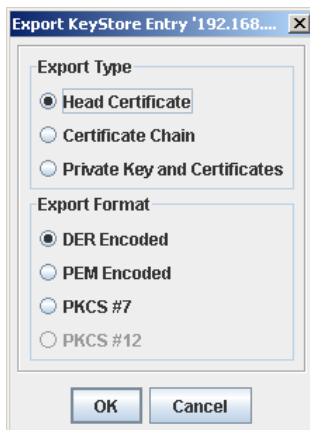


- d. Click **Tools->Generate Key Pair** and fill in the fields in the following dialog:

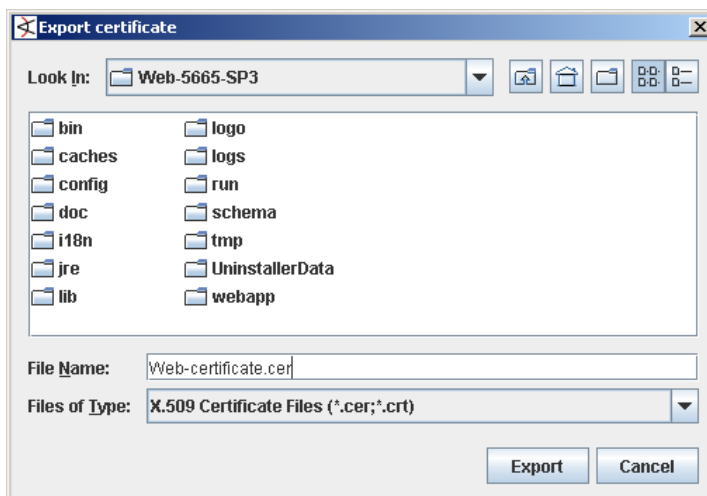
**Note:** Make sure to use the machine name or IP address on which ArcSight Web is installed for the CN name.



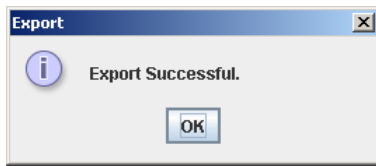
- e. Enter an alias for the key pair and click **OK**.
2. Export the key pair you just generated.
  - a. In the keytoolgui right-click the key pair you just generated and select **Export Key pair**.
  - b. Make sure to select **Head Certificate** as Export Type and **DER Encoded** as the Export Format in the following dialog and click **OK**:



- c. Enter a name for the certificate and click Export.



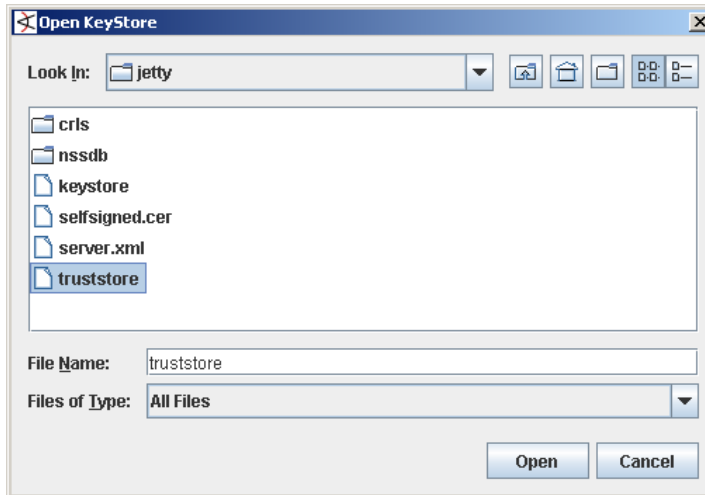
- d. You see the following message:



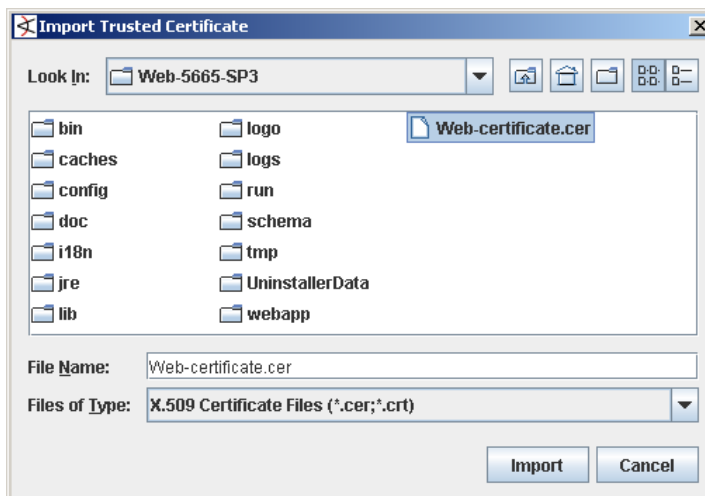
- e. If your ArcSight Web is on a different machine than the Manager, copy this certificate to the Manager's machine.
3. Save the keystore in the Web's <ARCSIGHT\_HOME>/config/jetty directory by clicking on **File->Save keystore**.
- a. Enter a password for the keystore and confirm it.



- b. Give the keystore a name and click **Save**.
4. If you are using self-signed certificate skip this step and continue with step 5.  
Import the signed certificate response in the keystore of ArcSight Web.
- Import the signed certificate response in the Web's keystore. Follow the steps in section “Import the CA Root Certificate”.
  - Use the changepassword tool to set an encrypted keystore password in the client.properties file:
- ```
arcsight changepassword -f config/client.properties -p
ssl.keystore.password
```
5. Add the following properties in the Web's <ARCSIGHT\_HOME>/config/client.properties file and save the file:
- ```
ssl.keystore.password=<password-set-when-you-saved-the-keystore>
ssl.keystore.path=config/jetty/webkeystore
```
6. Import Web's key pair into the Manager's truststore.
- If your Manager trusts the CA that signed your client's certificates, go to the next step. Otherwise perform these steps to update the Manager's truststore.
- a. Start the keytoolgui by entering `arcsight keytoolgui` command from the Manager's bin directory.
- b. Click **File->Open keystore** and navigate to <ARCSIGHT\_HOME>/config/jetty/truststore.



- c. Enter the password when prompted and click **OK**. For the default password see the “Keystore password” topic in the ESM Administrator’s Guide.
- d. Click **Tools->Import Trusted Certificate**.
- e. Navigate to the Web’s certificate that you exported earlier and click **Import**.



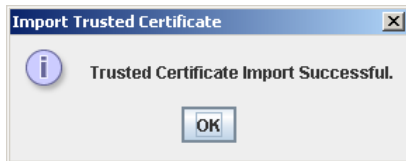
- f. You see the following message. Click **OK**.



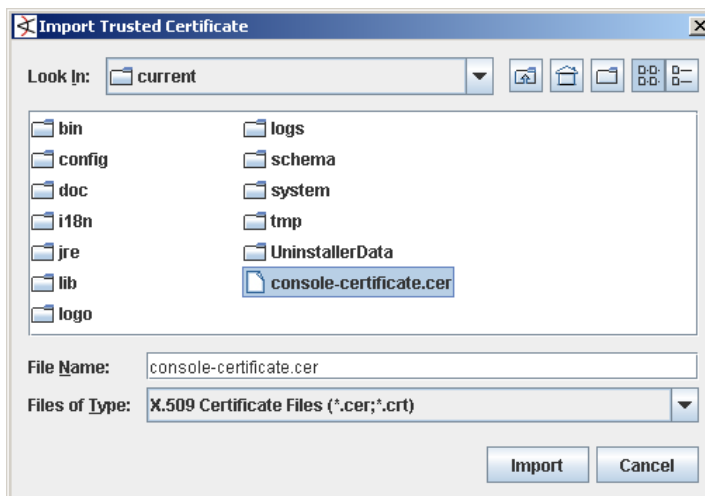
- g. Review the certificate details and click **OK**.
- h. Click **Yes** in the following dialog.



- i. Enter an alias for the certificate.
- j. You get the following message if the import was successful.



- k. Click **OK** and save the changes to the truststore.
7. Import Console's certificate into webtruststore.
- a. Start the keytoolgui from ArcSight Web's bin directory.
  - b. Click **File->Open keystore** and navigate to the Web's <ARCSIGHT\_HOME>/config/jetty/webtruststore.
  - c. Enter the password when prompted. For the default password see the topic “Keystore password” in the ESM Administrator's Guide.
  - d. Click **Tools->Import Trusted Certificate**.



- e. Navigate to the Console's certificate and click **Import**.
- f. Click **OK** in the next message box prompting you that “Could not establish a trust path for the certificate...”
- g. View the certificate details and click **OK**.
- h. Click **Yes** when prompted whether you want to accept the certificate as trusted.
- i. Enter an alias for the console's certificate and click **OK**.
- j. You see a message saying “Trusted Certificate Import Successful.”



- k. Click **OK**.
    - l. Save changes to the webtruststore and exit the keytoolgui.
8. Import the following into the web browser that you use with ArcSight Web:
  - Web’s certificate you exported in Step 2 of this procedure.
  - Console’s private key you created in Step 13 in section “Setting up Client-Side Authentication on ArcSight Console”.  
See your web browser’s documentation for steps to do the above.
9. Restart the Manager.
10. Restart ArcSight Web.

# 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 6.8c Patch 4)**

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](mailto:arc-doc@hpe.com).

We appreciate your feedback!