

---

# Micro Focus Security

## ArcSight ESM

Software Version: 6.11.0 Patch 3

### Release Notes

Document Release Date: September 30, 2018

Software Release Date: September 30, 2018



## Legal Notices

### Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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 2018 Micro Focus or one of its affiliates.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs</a>

# Contents

Welcome to ESM 6.11.0 Patch 3 .....	5
Important Prerequisite: Must Have Spectre and Meltdown Patches Applied .....	5
Purpose of this Patch .....	5
Upgrade Support .....	5
Vulnerability Updates .....	6
Geographical Information Update .....	6
Usage Notes .....	6
Uninstalling the Console Patch on the Mac .....	6
Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory ....	7
Authentication Between IE 11 and PKCS#11 Token .....	7
Correction to the Formula for Correlation Data Monitor .....	7
Variables on the ArcSight Command Center .....	8
Reference to SmartConnectors Not Updated (Customer URI) .....	9
SSL Client Authentication Not Available After Adding 6.11.0 Patch 3 .....	9
Silent Install is not Supported in Dark Theme for ESM 6.11.0 .....	9
Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations .....	10
Section 508 Compliance .....	10
Installing ESM Version 6.11.0 Patch 3 .....	10
Verifying the Downloaded Installation Software .....	11
If You Have the B7500 (G8) Appliance on RHEL 6.8 .....	11
ArcSight ESM Main Component Suite .....	12
To Install the Patch .....	12
After Patch Installation: RHEL 7.2 and 7.3 and CentOS 7.3 .....	14
To Uninstall the Patch .....	14
ArcSight Console .....	15
To Install the Patch .....	15
To Install the Patch on a Mac .....	17
To Uninstall the Patch .....	18
Fixed Issues .....	19
Analytics .....	19
ArcSight Console .....	20
ArcSight Manager .....	21
Command Center .....	22
General .....	22

Open and Closed Issues in ESM 6.11.0 Patch 1 and Patch 2 .....	23
Send Documentation Feedback .....	24

# Welcome to ESM 6.11.0 Patch 3

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

ESM includes the Correlation Optimized Retention and Retrieval (CORR) Engine, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

## Important Prerequisite: Must Have Spectre and Meltdown Patches Applied

As a prerequisite to installing ESM 6.11.0 Patch 3, you must have the patches for the Spectre and Meltdown vulnerabilities applied to your operating system.

## Purpose of this Patch

This patch:

- Updates the JRE to 1.8.0\_171-b11
- Addresses critical issues in ESM 6.11.0.
- Provides updates for geographical information and vulnerability mapping.
- Provides important security updates.
- Audit events are now generated by the creation or deletion of mark similar configurations. See "[Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations](#)" on page 10 for details.

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

## Upgrade Support

Apply this patch on ESM 6.11.0, with or without a released patch.

If you have older versions of ESM, upgrade those versions to 6.11.0 first before applying this patch.

For details on supported platforms, refer to the *ESM Support Matrix* available from the [Protect724 Community](#).

## Vulnerability Updates

This release includes recent vulnerability mappings from **Context Release Notes August 2018**.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2983	Faultline, Bugtraq, CVE, Nessus
Enterasys Dragon IDS	CVE
Cisco Secure IDS S1021	CVE
Juniper IDP update 3086	Faultline, Bugtraq, CVE, Nessus
TippingPoint UnityOne Dv9144	Faultline, MSSB
McAfee HIPS 7.0	CVE

## Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoLite2-City\_20180801.

## Usage Notes

### Uninstalling the Console Patch on the Mac

When uninstalling the Console Patch on the Mac, if the uninstall binary (Uninstall\_ArcSight\_ESM\_Console\_Patch) located in <CONSOLE\_HOME>/current/UninstallerData\_6.11.0.3 is used to uninstall the patch, then the UninstallerData\_6.11.0.3 directory is not deleted and the presence of this directory prevents reinstallation after the uninstall is done.

#### **Workaround:**

Use the symbolic link created when the patch was installed to invoke the Console Patch Uninstaller on the Mac, instead of the uninstall binary located in <CONSOLE\_HOME>/current/UninstallerData\_6.11.0.3. After deleting this directory, you can re-install the ArcSight Console ESM patch.

## Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory

An error occurs if you attempt to install the patch into the default /current directory on the Mac operating system. Instead, install into the root folder of the existing ESM 6.11.0 installation (for example, /Applications/arcsight\_611\_GA).

## Authentication Between IE 11 and PKCS#11 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.

## Correction to the Formula for Correlation Data Monitor

The ArcSight Console Guide has a topic, "Event Correlation Data Monitor." The formula is not correct. This usage note provides the correct formulas and explains how these formulas are used in the data monitor.

### How correlation is calculated

The event correlation data monitor applies covariance and correlation calculations to describe how two variables are related.

Covariance is calculated by the following formula:

$$COV(x,y) = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{n - 1}$$

where:

x is the independent variable

y is the dependent variable

$\bar{x}$  is the mean of the independent variable x

$\bar{y}$  is the mean of the dependent variable  $y$

Based on the covariance, correlation is then calculated by the following formula:

$$r(x, y) = \frac{COV(x, y)}{s_x s_y}$$

where:

$r(x, y)$  is the correlation of variables  $x$  and  $y$

$COV(x, y)$  is the covariance of variables  $x$  and  $y$

$s_x$  is the sample standard deviation of the random variable  $x$

$s_y$  is the sample standard deviation of the random variable  $y$

Correlation standardizes the measure of interdependence between two variables and, consequently, tells you how closely the two variables move. The correlation measurement, called a correlation coefficient, will always take on a value between 1 and -1:

- *If the correlation coefficient is 1*, the variables have a perfect positive correlation. This means that if one variable moves a given amount, the second moves proportionally in the same direction. A positive correlation coefficient less than one indicates a less than perfect positive correlation, with the strength of the correlation growing as the number approaches one.
- *If correlation coefficient is 0*, no relationship exists between the variables. If one variable moves, you can make no predictions about the movement of the other variable; they are uncorrelated.
- *If correlation coefficient is -1*, the variables are perfectly negatively correlated (or inversely correlated) and move in opposition to each other. If one variable increases, the other variable decreases proportionally. A negative correlation coefficient greater than -1 indicates a less than perfect negative correlation, with the strength of the correlation growing as the number approaches -1.

The data monitor sampler takes all samples in memory and continually calculates correlation values using this formula. As an example, you could define an event correlation data monitor that displays a correlation between the number of times a network is being reconnoitered, and if that is related to the number of attacks that the network is receiving.

## Variables on the ArcSight Command Center

The ArcSight Command Center does not support global and local variables. The ArcSight Command Center supports only standard event fields for viewing. Variables (global or local) are not supported. Use the ArcSight Console instead. See the following table:



## Fields

User Interface	Standard Event Fields	Local Variables	Global Variables
ArcSight Command Center	Yes	No	No
ArcSight Console	Yes	Yes	Yes

## Reference to SmartConnectors Not Updated (Customer URI)

When the customer object is renamed on the ArcSight Console, the associated reference to SmartConnectors (the Customer URI) is not updated with the new name. The Customer URI on the connector retains the old name. This is expected behavior and not an issue.

## SSL Client Authentication Not Available After Adding 6.11.0 Patch 3

After applying 6.11.0 Patch 3, the ArcSight Console in the Default-SSL console client does not connect to the Manager. The issue is that the Manager certificate is not in the client ArcSight Console truststore.

### Workaround:

Copy `jre.pre6.11.0.3\lib\security\cacerts` `jre\lib\security\cacerts`

## Silent Install is not Supported in Dark Theme for ESM 6.11.0

When in silent mode, the ESM Console installer does not trigger the `consolesetup` step at the end of the install. As a result, a default `console.properties` file is not generated during the installation. Dark theme requires access to this properties file.

### Workaround:

1. Run the `consolesetup` wizard in first in recording mode to capture a silent response file. For example:  

```
arcsight consolesetup -i recorderui -f console_silent.out
```
2. Use the response file `console_silent.out` to run `consolesetup` in silent mode. For example:  

```
arcsight consolesetup -i silent -f <full path to console_silent.out>
```

This results in a `config/console.properties` file in the ESM Console installation.
3. Now use the dark theme.

### Syntax:

Note that the `consolesetup` command supports the following parameters:

`consolesetup [-i <mode>] [-f <file>] [-g]`

### Parameters :

`-i <mode>` (modes are: console, silent, recorderui, swing)

`-f <file>` Log file name (properties file in `-i` silent mode)

`-g` (generate sample properties file for `-i` silent mode)

See the *ESM Administrator's Guide*, Appendix A: Administrative Commands for details on commands and parameters.

## Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations

The creation or deletion of mark similar configurations now generates audit events. You can add filters to view the audit events:

ID	Message	Priority
marksimilar:100	Mark similar configuration created	Low
marksimilar:102	Mark similar configuration removed due to time window expiry	Low
marksimilar:102	Mark similar configuration removed due to error. Check server.log	High
marksimilar:102	Mark similar - all have been removed	Medium

## 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.

## Installing ESM Version 6.11.0 Patch 3

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 3:

- As a prerequisite to installing ESM 6.11.0 Patch 3, you **must** have patches for the Spectre and Meltdown vulnerabilities applied to your operating system.
- **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 using 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

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

Visit the following site for information and instructions:

<https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do>

## If You Have the B7500 (G8) Appliance on RHEL 6.8

If you are upgrading from ESM 6.11.0 to 6.11.0 Patch 3 on a B7500 (G8) appliance with RHEL 6.8, and you do not want to upgrade the OS to RHEL 6.9, you must first install the standalone tzdata updater. Otherwise, the ESM 6.11.0 Patch 3 installer will display an error stating that you have an out-of-date tzdata package.

**Note:** If you are on RHEL 6.8, we recommend that you update to RHEL 6.9 before applying the patch. RHEL contains security fixes.

**The standalone tzdata updater is *not* required if you have one of these configurations:**

- ESM, software version
- ESM Express (G9) that has been upgraded to RHEL 7.5.
- ArcSight Express (G8) that has been upgraded to RHEL 6.9

**To install the tzdata updater on the B7500 appliance:**

1. Log in as **root**.
2. Go to the Micro Focus Software download site (<https://softwaresupport.softwaregrp.com/>)
3. Download the package `esm_tz_standalone_2018c.tar.gz` to a directory of choice on the appliance. In this example, we will use `/opt/upgrades`.
4. Go to `/opt/upgrades` and extract the archive with this command:

```
tar -xzf esm_tz_standalone_2018c.tar.gz
```

where `esm_tz_standalone_2018c` is a directory you designate.

5. Go to the new `<bundle_name>` directory, using our example:

```
cd /opt/upgrades/esm_tz_standalone_2018c
```

6. Run this command:

```
./tz_patch.sh
```

Wait for the message that confirms a successful update. In case of failures, the message will inform the reason, for example, unsupported platform or non-root user.

You can now proceed to the ESM 6.11.0 Patch 3 installation.

## ArcSight ESM Main Component Suite

This section describes how to install or uninstall the ESM 6.11.0 Patch 3 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, follow the steps in the subsection "To Uninstall the Patch" later in this section before installing the patch again.
- It is recommended 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 software download site (<https://softwaresupport.softwaregrp.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 page 11.

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

```
service 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:** Micro Focus 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 upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

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

```
service 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
```

## After Patch Installation: RHEL 7.2 and 7.3 and CentOS 7.3

After applying the patch, if the postgresql service becomes unavailable, check this log file:

```
/opt/arcsight/logger/userdata/logs/pgsql/serverlog
```

for the following messages:

```
FATAL: semctl(2162718, 14, SETVAL, 0) failed: Invalid argument  
FATAL: sorry, too many clients already
```

If you see these FATAL messages, perform the following steps:

1. As user **root**, edit the file `/etc/systemd/logind.conf`.
2. Search for `RemoveIPC`, and ensure there is only one instance of this property.
3. Edit the property if it exists (or add the property if it does not exist) to have the value **no**:

**RemoveIPC=no**

4. Run this command:

```
systemctl restart systemd-logind.service
```

## 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*:

```
service 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_6.11.0.3/UninstallerData_6.11.0.3` 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_6.11.0.3
```

Or, to uninstall using Console mode, run:

```
./Uninstall_ArcSight_ESM_Suite_Patch_6.11.0.3 -i console
```

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

4. When the uninstallation is complete press **Enter** to Exit.

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

```
service 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 6.11.0 Patch 3 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.
- It is recommended 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:** It is recommended 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 Software Support Online site (<https://softwaresupport.softwaregrp.com/>). YYYY.Y represents the Console build number.

- Patch-6.11.0.YYYY.Y-Console-Win.exe
- Patch-6.11.0.YYYY.Y-Console-Linux.bin
- Patch-6.11.0.YYYY.Y-Console-MacOSX.zip

Be sure to verify the patch file; see "[Verifying the Downloaded Installation Software](#)" 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-6.11.0.YYYY.Y-Console-Win.exe

- **On Linux:**

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

```
./Patch-6.11.0.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-6.11.0.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 upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

## 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. See the Usage Note ["Cannot Install ArcSight Console Patch for Mac Operating System into /current Directory" on page 7](#) for details.

**Note:** It is recommended 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-6.11.0.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 ["Verifying the Downloaded Installation Software" 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**.

**Note:** If you upgraded from 6.9.1c to 6.11.0, did you configure SSL Client Authentication using `keytoolgui` to generate keypairs and certificates?

If so, after completing patch installation at this step and before restarting services, regenerate the certificates.

## 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.

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 6.11.0 Patch 3 > Uninstall ArcSight ESM Console 6.11.0 Patch 3**

- Or, run the following from the Console's <ARCSIGHT\_HOME>\current\UninstallerData\_6.11.0.3 directory:

`Uninstall_ArcSight_ESM_Console_Patch.exe`

- On Windows 8.1, run the following from the Console's <ARCSIGHT\_HOME>\current\UninstallerData\_6.11.0.3 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_6.11.0.3`

- Or, to uninstall using Console mode, run:

`./Uninstall_ArcSight_ESM_Console_Patch_6.11.0.3 -i console`

- If you did not create a link, execute the command from the Console's <ARCSIGHT\_HOME>/current/UninstallerData\_6.11.0.3 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_6.11.0.3
```

- From the Console's <ARCSIGHT\_HOME>/current/UninstallerData\_6.11.0.3 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 3, 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.

• <a href="#">Analytics</a> .....	19
• <a href="#">ArcSight Console</a> .....	20
• <a href="#">ArcSight Manager</a> .....	21
• <a href="#">Command Center</a> .....	22
• <a href="#">General</a> .....	22

## Analytics

Issue	Description
NGS-27914	Reports that output the URL filename were not matching the ArcSight Console output. Fix: Reports no longer suppress the leading slash ( / ) to be consistent with the console.
NGS-27045	HTML reports embedded in email were not displaying Unicode Standard characters correctly. Fix: This issue has been fixed.

## ArcSight Console

Issue	Description
NGS-28088	<p>While using the custom Dark Theme, rendering of checkbox controls and rendering of a disabled label viewed in the Annotations Dialog, caused high CPU utilization. All OS platforms were affected.</p> <p>Fix: Two CPU usage issues with the ESM Console were fixed.</p>
NGS-27848	<p>Connector was not able to be upgraded if ESM was not registered as primary destination.</p> <p>Fix: A new console.properties option was added to the ESM Console in order to validate upgrade-related commands for Connectors. This flag is as follows:</p> <p># Setting this value to true will enable agent "primary" validation on upgrade and rollback upgrade commands.</p> <p>console.ui.agent.enable.upgradevalidation=false</p> <p>The default setting is "false". When the flag is set to "true", the ESM Console will ensure that a given Connector is considered a "primary" Connector for the current ESM Manager before enabling the "Upgrade" and "Rollback Upgrade" context menu options for the Connector. If the setting is "false", the previous behavior will keep the upgrade-related menu options enabled for primary and non-primary connectors.</p>

Issue	Description
NGS-26291	<p>Automatically-created connector filters were not removed when the filter was deleted.</p> <p>Fix: To enable removal of automatically created filters for agents, add the following property to the console.properties file:</p> <pre>console.ui.delete.agent.zone=true</pre>
NGS-25346	<p>User noticed incorrect position of India map in ArcSight console.</p> <p>Fix: The Console Geo map view now supports the following 3 options for specifying which Geo map to use as the background:</p> <p>In ESM Console, under - Edit --&gt; Preferences --&gt; Global Options</p> <p>There is a new row item called "Geo Map Type" with the following options:</p> <ol style="list-style-type: none"> <li>1) Countries</li> <li>2) Continents</li> <li>3) Custom</li> </ol> <p>"Countries" option is the currently used Geo world map and is the default. "Continents" option is a new Geo world map with no country borders and shows continents only. "Custom" is a new option that allows a user to specify their own custom shapefile when placed in the same directly location as the shapefiles for option 1) and 2). When "Custom" is selected, the Console will look for the shapefile based on the following console.properties specified setting:</p> <p>Setting this value is required when selecting the "Custom" Geo map type option from the user preferences.</p> <p>Specifies the filename ONLY.</p> <p>This file must be a valid shape file (*.shp) that resides in the following location: &lt;console_install_root_dir&gt;\Console\current\lib\resources\gisViews\</p> <pre>console.ui.geo.custom.mapfile=countries_edited.shp</pre> <p>In this instance, the user has placed the required shapefile "countries_edited.shp" in specified directory. The console attempts to use this shapefile as the Geo map background. If the console fails to load the specified custom file, an error is displayed and the default "Countries" Geo map is used instead. Users should also include any "*.dbf" same-named files as the *.shp" file in the specified directory.</p> <p>Note ArcSight does not provide custom maps.</p>

## ArcSight Manager

Issue	Description
NGS-27978	<p>Countries were labeled incorrectly for some IP addresses.</p> <p>Fix: This issue has been fixed.</p>
NGS-27664	<p>Multi-mapped active lists that contained a large number of entries under a single key in compact mode, could cause lists to load slowly and result in a long interval during manager startup.</p> <p>Fix: This issue has been fixed.</p>

## Command Center

Issue	Description
NGS-28148	<p>Maps in ArcSight console were shown in an incorrect position.</p> <p>Fix: The ACC Geo map now supports the option to change the map view between continent and countries.</p> <p>Under Admin list select Preference.</p> <p>A pop-up window will be displayed with a toggle button to turn on/off the option to show countries in the Geo Map.</p> <p>After you turn on/off this option, it is recommended to refresh or reload Geo Map Data Monitors to see the change immediately.</p> <p>Countries is currently the default used Geo world map. Continents is a new Geo world map with no country borders and it shows continents only. Once this option is switched, the user has to refresh the page or reload DM's containing Geo map.</p>
NGS-15018	<p>The ArcSight Command Center was showing End Time if the "Display Name" heading was not "End Time" in the query.</p> <p>Fix: End Time is now displayed in a readable format.</p>

## General

Issue	Description
NGS-28099	<p>Authentication with RADIUS was failing on ESM 6.11 if RADIUS had not been configured.</p> <p>Fix: This issue has been fixed.</p>
NGS-27505	<p>The Case Description field in ACC was omitting line breaks.</p> <p>Fix: This issue has been fixed.</p>
NGS-27289	<p>SNMPv1 traps were missing required header information.</p> <p>Fix: This issue has been fixed.</p>
NGS-27198	<p>New users could not be created when logged in through SSL authentication.</p> <p>Fix: This issue has been fixed.</p>
NGS-27015	<p>Some events with negative IDs were not displayed correctly in the console.</p> <p>Fix: This issue is now fixed.</p>
NGS-26994	<p>CustomConditionalEvaluation failed to recognize types in the ISNULL function leading to stemming errors from MySQL.</p> <p>Fix: The MySQL query was modified to avoid that behavior.</p>

Issue	Description
NGS-26651	REST API errors were not available for ACC pages; only blank pages were shown. Fix: REST API are now available for ACC pages.
NGS-26268	ESM crashed when users moved system-created stages to another folder. Fix: Issue has been fixed.
NGS-25671	Empty reports were not notified nor sent via email. Fix: Issue has been fixed. To disable, add the following to server.properties: report.scheduler.attach_empty_reports=false report.scheduler.notify_empty_reports=false
NGS-23242	Command line operations triggered by rule actions were not handling embedded quotes correctly. Fix: This issue has been fixed.
NGS-11751	When a group of assets was selected, unselected and then selected again, the folder tree did not show all categories. Fix: This issue has been fixed.

## Open and Closed Issues in ESM 6.11.0 Patch 1 and Patch 2

For information about open and closed issues for ESM 6.11.0 Patch 1 and Patch 2, see the release notes for those releases.

# 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 computer, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Release Notes (ESM 6.11.0 Patch 3)**

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 [arcsight\\_doc@microfocus.com](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!