Micro Focus Security ArcSight ESM

Software Version: 6.11 Patch 4

Release Notes

Document Release Date: April 2019
Software Release Date: April 2019

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 2019 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

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Welcome to ESM 6.11 Patch 4

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.

What's New in this Release

This patch addresses critical issues in ESM 6.11, provides support for new operating systems, and provides vulnerability and geographical information updates.

Support for New Operating Systems

This patch provides support for RHEL and CentOS 6.10 in traditional and high availability environments.

Vulnerability Updates

This patch includes the following vulnerability mappings from the February 2019 Context Update:

Device	Vulnerability update
Cisco Secure IDS S1025	CVE
Enterasys Dragon IDS	CVE
Juniper IDP update 3143	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
McAfee HIPS 7.0	CVE
McAfee Intrushield	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
Snort/Sourcefire SEU 2983	CVE, Bugtraq, X-Force
TippingPoint UnityOne DV9243	MSSB

Geographical Information Updates

This patch includes an update to the geographical information used in graphic displays. The version is GeoLite2-City_20190212.

Supported Upgrade Paths

You can apply this patch on ESM 6.11, with or without patches.

If you have an older version of ESM, upgrade to ESM 6.11, and then apply this patch.

Usage Notes

This section describes usage considerations that apply after you install this patch.

Section 508 Compliance

Micro Focus recognizes the importance of accessibility as a product initiative. Micro Focus continues to make advances in the area of accessibility in its ArcSight product lines.

Installing the ArcSight Console Patch on a Mac

ESM generates an error if you attempt to install this patch into the default `/current` directory on a Mac.

Instead, install this patch to the root folder of the existing ESM 6.11 installation (for example, `/Applications/arcsight_611_GA`).

Uninstalling the ArcSight Console Patch from a Mac

Do not use `Uninstall_ArcSight_ESM_Console_Patch` (located in `<CONSOLE_HOME>/current/UninstallerData_6.11.0.4` to uninstall the console patch from a Mac. The program does not delete the `UninstallerData_6.11.0.4` directory, which prevents you from being able to re-install the patch.

Instead, use the symbolic link that you created when you installed the patch.

Authentication Issue Between Internet Explorer 11 and PKCS#11 Token

In environments that use Internet Explorer 11 with ActivClient middleware and a PKCS#11 token, the following error occurs and users cannot log in to ArcSight Command Center:

```
This page can't be displayed
```

If you receive the error message, use another browser (for example, Firefox or Chrome), to authenticate the common access card (CAC). After you successfully authenticate the card through another browser, you can use the original browser without having to authenticate the card again.

Correction to the Formula for Correlation Data Monitor

The ArcSight Console User's Guide has an incorrect formula for calculating correlation. This section provides the correct formula.

The event correlation data monitor applies covariance and correlation calculations to describe the relationship between two variables. The data monitor uses the following formula to calculate covariance:

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

where:

x is the independent variable

y is the dependent variable

$\overline{x}$ is the mean of the independent variable *x*

$\overline{y}$ is the mean of the dependent variable *y*

Based on the covariance, the data monitor uses the following formula to calculate correlation:

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

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. 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 the 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.
- *If the 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 in ArcSight Command Center

ArcSight Command Center does not support global and local variables. It supports only standard event fields for viewing. If you need to use global or local variables, use the ArcSight Console.

Reference to SmartConnectors Not Updated (Customer URI)

When you rename a customer object in the ArcSight Console, ESM does not update the associated reference to SmartConnectors (the Customer URI) with the new name. The Customer URI on the connector retains the old name. This is expected behavior.

SSL Client Authentication Not Available After Applying 6.11 Patch 4

After you apply this patch, the ArcSight Console in the Default-SSL console client does not connect to the Manager because the Manager certificate is not in the client ArcSight Console truststore. To resolve this issue, use the following command:

```
Copy jre.pre6.11.0.4\lib\security\cacerts jre\lib\security\cacerts
```

Dark Theme not Supported with Silent Installation

If you install ESM in silent mode, the ArcSight Console installation program does not trigger the `consolesetup` step at the end of the installation and does not generate a `console.properties` file. The dark theme requires access to this properties file.

To resolve this issue:

1. Run the `consolesetup` wizard 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>
   ```

   The installation program creates a `config/console.properties` file and you can use the dark theme.

The `consolesetup` command supports the following parameters:

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

where:

mode is console, silent, recorderui, or swing

-file is the log file name (properties file in –i silent mode)

-g generates sample properties file for –i silent mode

For more information about commands and parameters, see the ESM Administrator's Guide.

Creating or Deleting Mark Similar Configurations Generates Audit Events

When you create or delete Mark Similar configurations, ESM 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

ID	Message	Priority
marksimilar:102	Mark similar configuration removed due to error. Check server.log	High
marksimilar:102	Mark similar - all have been removed	Medium

Installing ESM Version 6.11 Patch 4

To install this patch, use the platform-specific component executable files that are included. Patch installers are available for all supported platforms.

The ArcSight Console has separate installation and uninstallation procedures.

Keep the following points in mind:

- Ensure that you have enough space available *before* you install the patch. The installation program checks for 1 GB of space and generates an error if it is not available. If you have disk space issues during installation, create enough space, restore the component base build from the backup, and then resume patch installation.
- Backup, installation, and uninstallation procedures require permissions for the relevant components. To install the patch, ensure 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 have the same user level as the original installer.
- Micro Focus recommends creating a backup of the existing product before installation. Do not rename files and leave them in the same directory. Java reads all of the files present, regardless of renaming, and can inadvertently pick up old code, causing undesirable results.
- For backup, patch installation, and uninstallation, Micro Focus recommends that you log in to the target computer using SSH. If you switch accounts after logging in, specify the flag "-" for the `su` command (`su - <User_Name>`).

Caution: Do not interrupt the patch installation process (for example, do not press Ctrl-C or log off). Interrupting the process causes undesirable results.

Verifying the Downloaded Installation Software

After you download the software, contact Micro Focus ArcSight Support to verify that the signed software is from Micro Focus and has not been manipulated by a third party.

Installing this Patch on a B7500 (G8) Appliance on RHEL 6.8

If you are installing this patch on a B7500 (G8) appliance with Red Hat Enterprise Linux (RHEL) 6.8 and do not want to upgrade the operating system to RHEL 6.9, you must first

install the standalone tzdata updater. Otherwise, the patch installation program will generate an error stating that you have an out-of-date tzdata package.

Note: Because RHEL 6.9 includes security fixes, Micro Focus recommends that you upgrade the operating system to RHEL 6.9 before you apply this patch.

The following configurations do not require the standalone tzdata updater:

- ESM Software
- 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, access the Micro Focus software download site, and download the `esm_tz_standalone_2018g.tar.gz` package to the desired directory on the appliance. For example, `/opt/upgrades`.
2. Navigate to the download directory and enter the following command to extract the archive:

   ```
   tar -xzf <ESM_tz_Standalone_2018g>.tar.gz
   ```

   where `ESM_tz_Standalone_2018g` is a directory that you designate.
3. Navigate to the new directory. For example:

   ```
   cd /opt/upgrades/ESM_tz_standalone_2018g
   ```
4. Enter the following command:

   ```
   ./tz_patch.sh
   ```

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

You can now install this patch.

Installing this Patch on the ESM Main Components

This section describes how to install ESM 6.11 Patch 4 for all components except the ArcSight Console. These components include the Manager and the CORR-Engine.

Keep the following points in mind:

- Verify that open shells are not accessing the `<ArcSight_Home>` directory or any of its subdirectories.
- If you need to re-install this patch, first uninstall it and then install it again.

To install this patch:

1. Download `ArcSightESMSuitePatch-XXXX.tar` from the Micro Focus software download site, where XXXX is the suite build number.
2. As user arcsight, extract the `.tar` file.
3. As user arcsight, stop the ArcSight services:

   ```
   service arcsight_services stop all
   ```
4. Make a copy of the `/opt/arcsight` directory and place it in a readily accessible location.

   This is a precautionary measure so that you can restore the system to the original state, if necessary.
5. If you are installing this patch in a high availability environment, run the following command on the secondary server as user root to place the server in standby mode:

   ```
   crm_standby -v true
   ```
6. From the directory where you extracted the `.tar` file, run the patch installation program as user arcsight:

   ```
   ./ArcSightESMSuitePatch.bin
   ```

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

   ```
   ./ArcSightESMSuitePatch.bin -i console
   ```
7. If you want a shortcut to the uninstallation program in a different location, select a location for the link.

   You must have write permission to the folder that you specify.
8. Verify that the pre-installation summary is correct, and then press **Enter**.
9. After the installation is complete, start the ArcSight services as user arcsight:

   ```
   service arcsight_services start all
   ```
10. In a high availability environment, run the following command on the secondary server as user root to bring the server online:

    ```
    crm_standby -D
    ```

Uninstalling this Patch From the Main Components

If needed, use the procedure below to uninstall this patch and restore the system to the original state.

Note: Before you uninstall, verify that open shells are not accessing the Manager's `<ArcSight_Home>` directory or any of its subdirectories.

To uninstall this patch:

1. As user arcsight, stop the ArcSight services:

   ```
   service arcsight_services stop all
   ```
2. In a high availability environment, run the following command on the secondary server as user root to place the server in standby mode:

   ```
   crm_standby -v true
   ```
3. As user arcsight, run the uninstallation program from either the directory where you created the link when you installed the patch or, if you did not create a link, from the `/opt/arcsight/suitepatch_6.11.0.4/UninstallerData_6.11.0.4` directory:

   ```
   ./Uninstall_ArcSight_ESM_Suite_Patch
   ```

   To uninstall in Console mode, run the following command:

   ```
   ./Uninstall_ArcSight_ESM_Suite_Patch_6.11.0.4 -i console
   ```
4. After the uninstallation is complete, start the ArcSight services as user arcsight:

   ```
   service arcsight_services start all
   ```
5. In high availability environments, run the following command on the secondary server as user root to bring the server online:

   ```
   crm_standby -D
   ```

Installing this Patch on the ArcSight Console

This section describes how to install the ESM 6.11 Patch 4 for ArcSight Console on Microsoft Windows, Mac, and Linux platforms.

Note: The ArcSight Console is not supported on AIX and Solaris platforms.

Keep the following points in mind:

- Verify that open shells are not accessing the `<ArcSight_Home>` directory or any of its subdirectories.
- If you need to re-install this patch, first uninstall it and then install it again.

To install this patch on Windows or Linux:

1. Exit the ArcSight Console.
2. Make a copy of the console directory (for example, `/home/arcsight/console/current`) and place it in a readily accessible location.

   This is a precautionary measure so that you can restore the system to the original state, if necessary.
3. Download the executable file specific to your platform from the Micro Focus software

download site, where YYYY is the console build number:

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

4. If you are installing this patch on Windows, run Patch-6.11.0.YYYY.Y-Console-Win.exe.
5. If you are installing this patch on Linux, run the following command as user arcsight:

   ./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:

   ./Patch-6.11.0.YYYY.Y-Console-Linux.bin -i console
6. Select the location of the existing <ArcSight_Home> directory for the console installation.

   To restore the default location that the installation program provided, select **Restore Default Folder**.
7. Select a link location (on Linux) or shortcut location (on Windows).
8. Verify that the pre-installation summary is correct, and then press **Enter**.

To install this patch on a Mac:

1. Exit the ArcSight Console.
2. Make a copy of the console directory (for example, /home/arcsight/console/current) and place it in a readily accessible location.

   This is a precautionary measure so that you can restore the system to the original state, if necessary.
3. Download Patch-6.11.0.YYYY.Y-Console-MacOSX.zip from the Micro Focus software download site, where YYYY is the console build number.

   Tip: The patch installation file has a .zip extension on the download site, but a .app extension when you download it to a Mac. You do not need to extract or unzip the file.
4. Double-click the ArcSightConsolePatch.app file.
5. Follow the prompts in the patch installation wizard.
6. Verify the settings, and then click **Install**.

Uninstalling this Patch from the ArcSight Console

If needed, use the procedure below to uninstall this patch and restore the system to the original state.

Note: Before you uninstall, verify that open shells are not accessing the `<ArcSight_Home>` directory or any of its subdirectories.

1. Exit the ArcSight Console.
2. Run the uninstallation program:

On this platform:	Do this:
Windows	Use one of the following methods: • Double-click the icon that you created for the uninstallation program when you installed the console. • Use the link that you created in the **Start** menu. • Run `Uninstall_ArcSight_ESM_Console_Patch.exe` from `<ArcSight_Home>\current\UninstallerData_6.11.0.4`.
Linux	Use one of the following methods: • From the directory where you created the link when you installed the console, run `./Uninstall_ArcSight_ESM_Console_Patch_6.11.0.4`. To uninstall in Console mode, run `./Uninstall_ArcSight_ESM_Console_Patch_6.11.0.4 -i console`. • From the `<ArcSight_Home>/current/UninstallerData_6.11.0.4` directory on the console computer, run `./Uninstall_ArcSight_ESM_Console_Patch`. To uninstall in Console mode, run `./Uninstall_ArcSight_ESM_Console_Patch -i console`.
Mac	From the directory where you created the link when you installed the console, run `Uninstall_ArcSight_ESM_Console_Patch_6.11.0.4`.

Fixed Issues

The section provides information about issues that are fixed in this release.

ArcSight Console

Issue	Description
NGS-22636	This patch resolves an issue where if you edited multiple resources of the same type (for example, rules) and having the same name and then canceled a modification, ESM automatically closed the first tab that you opened rather than the active tab.
NGS-26519	This patch resolves an issue where integration commands that were based on event field type were not available for use in the console.
NGS-28200	This patch resolves an issue where it was not possible to create rules with the characters "/n" in text fields. ESM did not trigger the rules.

ArcSight Manager

Issue	Description
NGS-24623	This patch resolves an issue where using five-digit emoticon codes for the Destination User Name value resulted in some events not displaying in active channels and "Incorrect string value" errors when running reports.

CORR-Engine

Issue	Description
NGS-21573	This patch resolves an issue where IP comparisons in the Rules Editor were non-associative.

Reports

Issue	Description
NGS-26777	This patch resolves an issue where the `$Custom<parameter_name>` parameter did not work with report templates. ESM did not replace the parameter name with the parameter value in reports.

General

Issue	Description
NGS-28528	This patch resolves an issue where the following properties were missing from `manager/config/server.defaults.properties`: • `#ssl.protocols.nonfips=SSLv2Hello,TLSv1.2` • `#ssl.protocols=TLSv1.2` By default, the properties are disabled. If you enable them, you must use the values that are shown above.

Open and Closed Issues in Previous Releases

For information about open and closed issues for ESM 6.11 Patch 2, see the Release Notes.

For information about open and closed issues for ESM 6.11 Patch 3, see the Release Notes.

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 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 arcsight_doc@microfocus.com.

We appreciate your feedback!