
Micro Focus Security ArcSight ESM

Software Version: 7.0 Patch 2

Release Notes

Document Release Date: April 2, 2019

Software Release Date: April 2, 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 7.0 Patch 2	5
What's New in this Release	5
Vulnerability Updates	6
Geographical Information Updates	6
Unsupported Features in this Release	7
Usage Notes	8
90Meter Cards and Firefox Browser	8
Actor Model Import Connector	8
Asset Model Import FlexConnector	8
Forwarding Connector	9
Distributed Correlation Mode	9
Optimal Active List Configuration	11
Section 508 Compliance	11
Session List Overflow	11
Support for ActivClient Issues	12
Supported Versions for Distributed Searches	13
X Window System on Linux Computers	13
Installing ESM Version 7.0 Patch 2	15
Verifying the Downloaded Installation Software	16
Installing the ESM Main Components	16
Uninstalling this Patch From the Main Components	18
Installing the ArcSight Console	19
Uninstalling this Patch from the ArcSight Console	21
Resolved Issues	22
Analytics	22
ArcSight Console	22
ArcSight Manager	23
Command Center	24
Connectors	24
CORR-Engine	24
General	25
Open Issues	26
Command Center	26
ArcSight Console	26
Correlation	27

Manager	27
Open and Closed Issues in Previous Releases	28
Send Documentation Feedback	29

Welcome to ESM 7.0 Patch 2

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 includes several enhancements.

ArcSight Console

This patch includes the following enhancements to the ArcSight Console:

- Improvements to ServiceNow® integration

When exporting a case to ServiceNow® IT Service Management, the default value for the **Caller ID** field is the currently logged in ServiceNow® user. To change the caller ID, you can select from a drop-down list of recent selections or begin typing in the drop-down field and select from a list of matching values.

The **Assigned To** and **Assignment Group** fields also provide the same drop-down functionality.

For information about ServiceNow® integration, see the [ArcSight Console User's Guide](#).

- Display maps in the background

ArcSight ESM now includes a global option that allows you to display a world map with country borders, a world map without country borders, or a custom map in the background.

By default, ESM displays a world map with country borders. To change the default setting, select **Edit > Preferences > Global Options**, select the desired setting for the **Geo Map Type** global option, and then select **Use classic charts**.

If you select **Custom** as the map type, you must place a valid shape file (.shp) and any associated .dbf files in <Console_Installation_Directory>\Console\current\lib\resources\gisViews\ and you must edit the console.properties file in <Console_Installation_Directory>\current\config to

reference the shape file. For example:

```
console.ui.geo.custom.mapfile=my_map.shp
```

After you edit the `console.properties` file, restart the console for the changes to take effect.

For information about editing the `console.properties` file, see the [ESM Administrator's Guide](#).

Command Center

Command Center now includes the option to switch from the default country geo map to a continent geo map.

To switch to a continent geo map:

1. On the main page, hover over **admin** and then select **Preferences**.
2. Turn off the option to display country geo maps.
3. Refresh the geo map data monitors.

Vulnerability Updates

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

Device	Vulnerability update
Cisco Secure IDS S1024	CVE
Enterasys Dragon IDS 20190108	CVE
Juniper IDP update 3131	CVE, Bugtraq
McAfee HIPS 7.0/8.0 content version 8807	CVE
McAfee Intrushield 9.8.31.1	Faultline, Bugtraq, CVE, Nessus
Snort/Sourcefire 2983	CVE, Bugtraq
TippingPoint UnityOne DV9217	MSSB

Geographical Information Updates

This patch includes an update to the geographical information used in graphic displays. The version is GeoLite2-City_20181001.

Unsupported Features in this Release

This information applies to ESM Software and ESM Express with ESM 7.0 Patch 2:

- Multi-mapped active lists with over 10,000 entries per key are not supported.
- Large partially cached active lists are not supported.

Usage Notes

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

90Meter Cards and Firefox Browser

If you are using Firefox version 45.1.1 with 90Meter cards for authentication, you might receive an error stating that `x86\l1tpkcs11.dll` is not supported. For information about configuring Firefox to resolve this issue, contact the 90Meter vendor.

Caution: Do not use Firefox versions 45 and later with Windows 8.1 Enterprise. Instead, use Firefox 38.0.1 ESR.

For more information about 90Meter card support, see the [ESM Support Matrix](#).

Actor Model Import Connector

The Actor Model Import Connector for Microsoft Active Directory allows you to develop a model import connector to import actor model data. You can configure the connector in a dual stack or pure IPv6 environment. For more information, see the [Actor Model Import Connector for Microsoft Active Directory Configuration Guide](#).

Use Actor Model Import Connector version 7.9.0.8085.0 with this patch. Do not use previous versions of the connector with this patch.

Asset Model Import FlexConnector

The Asset Model Import FlexConnector allows you to develop a model import connector to import asset model data from a file, create and maintain ESM network model data, and synchronize it with the data in your asset management system. You can configure the connector in a dual stack or pure IPv6 environment. For more information, see the [Asset Model Import FlexConnector Developer's Guide](#).

Use Asset Model Import FlexConnector version 7.9.0.8086.0 with this patch. Do not use previous versions of the connector with this patch.

Forwarding Connector

The ArcSight Forwarding Connector receives events from a source Manager and sends them to a secondary destination Manager, ArcSight Logger, or a non-ESM destination. The connector can forward events with IPv4 or IPv6 addresses. If the destination supports both IPv4 and IPv6 addresses, ESM uses address fields such as Attacker, Source, and Target. If the destination does not support IPv6 addresses, ESM uses the deviceCustomIPv6Address fields. For more information, see the [Forwarding Connector Configuration Guide](#).

Use Forwarding Connector version 7.9.0.8087.0 with this patch. Do not use previous versions of the connector with this patch.

Distributed Correlation Mode

The following usage notes apply to ESM running in distributed correlation mode.

Requirements for Installing this Patch

When you install this patch, you must install it on all cluster nodes. If the nodes are not the same version, you will experience serious issues.

XML-RPC Requests

To reduce the number of XML-RPC requests that ESM sends when running in distributed correlation mode, you can configure the distributed cache (dcache) service to handle some of the requests using stored data. The following policies are available:

- **EXECUTE**
ESM executes all requests as direct calls to the persistor. This policy uses the most resources. Micro Focus recommends this policy only in environments where category assignments change frequently.
- **DCACHE4SELECTED**
If the requested values are present in dcache, ESM uses dcache to fulfill requests from data monitors. For all other tasks (for example, requests from rules and filters), ESM executes requests as direct calls to the persistor. This policy is set by default.
- **DCACHE**
ESM firsts checks the values in dcache to fulfill requests and only sends an XML-RPC request if it does not find data in dcache.

To change the method for handling XML-RPC requests:

1. On the dcache node, type the following command to determine the method currently in use:

```
bin/arcsight rtprops -c list
```

2. To change the method, type the following command:

```
bin/arcsight rtprops -c set -p "arcsight.corr.category.function.policy" -v  
<Policy_Name>
```

where Policy_Name is EXECUTE, DCACHE4SELECTED, or DCACHE

By default, entries in dcache have a time-to-live (TTL) timeout of 15 minutes (900 seconds). When an entry reaches the timeout value, dcache automatically removes it, regardless of whether it was recently used. You can change the default timeout value.

To change the timeout value for entries in dcache:

1. On the dcache node, type the following command:

```
<ArcSight_Home_Directory>/bin/arcsight dcachesetup
```
2. Select **Configure Common Settings**.
3. Change the TTL value to the desired number of seconds.
4. Restart all dcache instances.

Active List Updates in Distributed Correlation

If a rule includes the condition NOT In ActiveList and an action to add the relevant data to the active list that the rule is evaluating, the rule might trigger excessively. Consider other options such as using the OnFirstEvent trigger instead of the OnEveryEvent trigger.

If you have a pair of rules where the first rule populates a list and the second rule depends on data being in that list, and both rules are expected to operate on the same event, the first rule might not update the list in time for the second rule to trigger as expected.

Because the order of rule processing is not guaranteed, you might also experience issues with this scenario in compact mode. Even if both rules are not expected to operate on the same event, if the events arrive too closely together, ESM might not trigger the second rule because the active list has not been updated.

Recommended Cluster Configurations

When installing ESM in distributed correlation mode, configure a minimum of four nodes and no more than five nodes. For more information about configuring four- and five-node clusters, see the [ESM Installation Guide](#).

Performance Tuning

When using ESM in distributed correlation mode, the default capacity of internal buffers that temporarily store incoming events might limit persistence throughput. If the incoming

event rate is greater than 25,000 events per second (EPS), add the following lines to the `server.properties` file, and then restart the ESM cluster:

```
queue.logger.pre-security-event-persistor.capacity=200000  
queue.logger.start-of-flow.capacity=200000
```

For information about editing the `server.properties` file, see the [ESM Administrator's Guide](#).

Optimal Active List Configuration

ESM removes entries from active lists in the following situations:

- The entries reach the time-to-live (TTL) value that you specified (the entries expire).
- The active list reaches the maximum capacity (ESM evicts the entries).

For optimal performance, configure active lists to cause entries to expire rather than be evicted. To prevent ESM from evicting entries, active lists should have a capacity that is sufficient to hold the entries during their TTL. Determine the average insertion rate, and then multiply the insertion rate by the TTL value and add a percentage of slack to account for periods of increased traffic. For example:

$\text{active list capacity} = \text{insertion rate} * \text{TTL} * 1.5$

The example uses a slack of 50 percent. You might need a larger percentage if your environment is subject to frequent increases in traffic.

For more information about configuring active lists, see the [ArcSight Console User's Guide](#).

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.

Session List Overflow

Session list overflow occurs when there are more open sessions in the list than can be held in memory. In an overflow state, a session list behaves like a partially cached active list, where any lookup can result in a database hit. This functionality does not work in distributed mode for either active lists or session lists. Because you cannot disable this functionality for session lists, it is important to balance the capacity and input rate of entries to a given list. You can take the following actions to avoid session list overflow:

- Increase the list In MemoryCapacity.
- Set the expiration time so that ESM automatically terminates entries before overflow occurs.
- Modify rule conditions to restrict the events that generate entries.
- Reduce the number of input events that cause a new list entry. Instead of including all types of events when increasing events per second (EPS), be aware of which events might cause unreasonable list growth and limit those.
- Break up the list so that multiple lists hold different parts of the original list (for example, by IP range).

In addition to avoiding session list overflow, it is important to keep the database table from getting too large. Because session lists can be partially cached, it is possible for them to grow much larger in the database. If you do not manually delete entries from the database, configure the lists with a time-to-live (TTL) value so that ESM periodically deletes closed entries. For information about setting the TTL value, see the [ArcSight Console User's Guide](#).

Support for ActivClient Issues

This information applies in environments that use ActivClient and common access cards (CACs) for ESM authentication. If your environment uses versions of ActivClient and CACs that Micro Focus has not tested, you might experience problems.

ActivClient releases are typically more frequent than ESM releases. In case of ActivClient issues, contact the ActivClient vendor. If you would like Micro Focus ArcSight Support to assist with monitoring the resolution or opening a ticket with ActivClient Support, ActivClient requires documentation stating that you are providing permission to ArcSight Support to assist with monitoring the ActivClient case. Send the permission to Micro Focus through email.

US Government customers can send an email to support-usa@actividentity.com to open a ticket.

Other customers can send an email to support@actividentity.com to open a ticket.

ActivClient Support typically requires the following information when you open a ticket:

- Attach the ActivClient logs and diagnostics in the AI incident for review. The AI team sends these logs to their Engineering team in France. They require permission to view the log files (as per CFIUS requirements).
- Collect any error messages and a Java console capture.
- Provide findings from Advanced Diagnostics:
 - a. Insert the SmartCard.
 - b. Right-click the **ActivClient** icon in the lower right system tray.

- c. Select **Advanced Diagnostics**.
 - d. Click **Diagnose** with the SmartCard inserted, and wait for the diagnostics to complete.
 - e. Select **File > Save As** to save the information to a file.
 - f. Include the file with your ActivClient support request.
- Provide information from the ActiveClient logs:
 - a. Open the ActivClient Console.
 - b. Select **Tools > Advanced > Enable Logging**.
 - c. Note the location of the log files. The files are typically in C:\Program Files\Common Files\ActivIdentity\Logs or C:\Program Files (x86)\Common Files\ActivIdentity\Logs.
 - d. Restart the computer.
 - e. Reproduce the issue.
 - f. Include all files generated in the logging directory with your ActivClient support request.

Important: As claimed by the vendor, generated log files that you provide to ActivClient Support do not contain personal information that is considered sensitive. Consult the vendor to ensure that the content does not include private information. For example, you should know what types of information are considered sensitive, and therefore not traced.

Supported Versions for Distributed Searches

Distributed searches are supported only on ESM peers of the same version.

IPv6 connectivity and IPv6 data search are supported on ESM versions 6.11.0 and above.

For more information about distributed searches, see the [Command Center User's Guide](#).

X Window System on Linux Computers

After you log in to the console on Linux computers running X Window System, the console might stop unexpectedly with the following error message:

Gdk-ERROR **: The program '<unknown>' received an X Window System error. This probably reflects a bug in the program.

This issue is not common. If it occurs, the workaround is to delete <User_Name>.ast and log in to the console again.

The <User_Name>.ast file is located in the home directory of the console installation. For example, /home/arcsight/console/current.

Installing ESM Version 7.0 Patch 2

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.

Caution: Before upgrading from ESM 7.0 to ESM 7.0 P2 in a high availability environment, users must install the High Availability hotfix HA_Hotfix-700-NGS-27665. For information about obtaining this hotfix, [contact Micro Focus ArcSight Support](#).

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 temporary 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.

If you are running ESM 7.0 in a high availability environment, after you install the patch, you can download and install an updated High Availability Monitoring Package. The package is available on [Micro Focus Marketplace](#).

If you are running ESM 7.0 Patch 1, you do not need to update the High Availability Monitoring Package.

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 the ESM Main Components

This section describes how to install ESM 7.0 Patch 2 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.

Procedures for installing in compact mode and distributed mode are different.

To install this patch in compact mode:

1. Download ArcSightESMSuitePatch-7.0.0.XXXX.2.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:

```
/etc/init.d/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. As user root, run the following command:
`/opt/arcsight/suite/bin/scripts/runAsRoot.sh`
10. After the installation is complete, start the ArcSight services as user arcsight:
`/etc/init.d/arcsight_services start all`
11. In a high availability environment, run the following command on the secondary server as user root to bring the server online:
`crm_standby -D`

To install this patch in distributed correlation mode:

Caution: You must first install this patch on all nodes *except* the persistor node. After you complete the installation on the non-persistor nodes, install this patch on the persistor node.

1. Use ArcSight Command Center to set the backpressure mode to **On** so that the event flow stops and ESM processes the incoming events in the cluster.
 When the correlator and aggregator lags reach 0, you can shut down the system.
 For more information, see the [ArcSight Command Center User's Guide](#).
2. Download ArcSightESMSuitePatch-7.0.0.XXXX.2.tar from the [Micro Focus software download site](#), where XXXX is the suite build number.
3. As user arcsight, extract the .tar file.
4. On the persistor node, as user arcsight, stop the ArcSight services:
`/etc/init.d/arcsight_services stop all`
5. For each node *except* the persistor node, 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`
6. 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.
7. Verify that the pre-installation summary is correct, and then press **Enter**.
8. As user root, run the following command:
`/opt/arcsight/suite/bin/scripts/runAsRoot.sh`
9. On the persistor node, 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
```

10. 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.

11. Verify that the pre-installation summary is correct, and then press **Enter**.

12. As user root, run the following command:

```
/opt/arcsight/suite/bin/scripts/runAsRoot.sh
```

13. As user arcsight, start the ArcSight services:

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

14. Use ArcSight Command Center to set the backpressure mode to **Auto**.

Uninstalling this Patch From the Main Components

If needed, use the applicable procedure below to uninstall this patch and restore the system to the original state. Procedures for uninstalling in compact mode and distributed mode are different.

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 in compact mode:

1. As user arcsight, stop the ArcSight services:

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

2. As user root, run the following command:

```
/opt/arcsight/suite/bin/scripts/runAsRoot.sh -u
```

3. 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
```

4. 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_7.0.0.2/UninstallerData_7.0.0.2 directory:

```
./Uninstall_ArcSight_ESM_Suite_Patch
```

To uninstall in Console mode, run the following command:

```
./Uninstall_ArcSight_ESM_Suite_Patch_7.0.0.2 -i console
```

5. After the uninstallation is complete, start the ArcSight services as user arcsight:

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

6. In high availability environments, run the following command on the secondary server as user root to bring the server online:

```
crm_standby -D
```

To uninstall this patch in distributed correlation mode:

1. Use ArcSight Command Center to set the backpressure mode to **On** so that the event flow stops and ESM processes the incoming events in the cluster.

When the correlator and aggregator lags reach 0, you can shut down the system.

For more information, see the [ArcSight Command Center User's Guide](#).

2. For each node *except* the persistor node, run the following command as user root:

```
/opt/arcsight/suite/bin/scripts runAsRoot.sh -u
```

3. On the persistor node, stop the ArcSight services as user arcsight:

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

4. For each node *except* the persistor node, change directory to `/opt/arcsight/suitepatch_7.0.0.2/UninstallerData_7.0.0.2` and then run `Uninstall_ArcSight_ESM_Suite_Patch` as user arcsight.

5. On the persistor node, run the following command as user root:

```
/opt/arcsight/suite/bin/scripts runAsRoot.sh -u
```

6. On the persistor node, change directory to `/opt/arcsight/suitepatch_7.0.0.2/UninstallerData_7.0.0.2` and then run `Uninstall_ArcSight_ESM_Suite_Patch` as user arcsight.

7. As user arcsight, start the ArcSight services:

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

8. Use ArcSight Command Center to set the backpressure mode to **Auto**.

Installing the ArcSight Console

This section describes how to install the ESM 7.0 Patch 2 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-7.0.0.YYYY.2-Console-Win.exe`
 - `Patch-7.0.0.YYYY.2-Console-Linux.bin`
4. If you are installing this patch on Windows, run `Patch-7.0.0.YYYY.2-Console-Win.exe`.
5. If you are installing this patch on Linux, run the following command as user arcsight:
`./Patch-7.0.0.YYYY.2-Console-Linux.bin`
To install in Console mode, run the following command from the shell prompt and then follow the instructions:
`./Patch-7.0.0.YYYY.2-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-7.0.0.YYYY.2-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	<p>Use one of the following methods:</p> <ul style="list-style-type: none"> • 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 <code>Uninstall_ArcSight_ESM_Console_Patch.exe</code> from <code><ArcSight_Home>\current\UninstallerData_7.0.0.2</code>.
Linux	<p>Use one of the following methods:</p> <ul style="list-style-type: none"> • From the directory where you created the link when you installed the console, run <code>./Uninstall_ArcSight_ESM_Console_Patch_7.0.0.2</code>. To uninstall in Console mode, run <code>./Uninstall_ArcSight_ESM_Console_Patch_7.0.0.2 -i console</code>. • From the <code><ArcSight_Home>/current/UninstallerData_7.0.0.2</code> directory on the console computer, run <code>./Uninstall_ArcSight_ESM_Console_Patch</code>. To uninstall in Console mode, run <code>./Uninstall_ArcSight_ESM_Console_Patch -i console</code>.
Mac	<p>Use one of the following methods:</p> <ul style="list-style-type: none"> • From the directory where you created the link when you installed the console, run <code>Uninstall_ArcSight_ESM_Console_Patch_7.0.0.2</code>. • From the <code><ArcSight_Home>/current/UninstallerData_7.0.0.2</code> directory on the console computer, run <code>Uninstall_ArcSight_ESM_Console_Patch</code>.

Resolved Issues

The section provides information about issues that are fixed in this release or resolved with a workaround.

Analytics

Issue	Description
NGS-27377	<p>Because the CORR-Engine receives events in batches, a batch that includes large events might impact performance.</p> <p>Workaround: To allow ESM to dynamically adjust the batch size, add the following property to the <code>server.properties</code> file:</p> <pre>packer.chunk-split-optimization=true</pre> <p>For information about editing the <code>server.properties</code> file, see the ESM Administrator's Guide.</p>
NGS-28134	<p>This patch resolves an issue where ESM incorrectly formatted HTML reports that were embedded in emails and encoded with UTF-8.</p>

ArcSight Console

Issue	Description
NGS-8185	<p>This patch resolves an issue where ESM generated an exception when you selected a local variable from the drop-down list for the Set Event Field action in rules.</p>
NGS-28082	<p>This patch resolves an issue where if you selected the Use classic charts option in Global Preferences to change the layout of a data monitor that you added to a dashboard, the console did not retain the settings after you saved and closed the dashboard.</p>

Issue	Description
NGS-28206	This patch resolves an issue where filter labels and values were not visible in active channel views under certain sizing scenarios.
NGS-28384	<p>New charts are limited to a maximum of 20 results.</p> <p>Workaround: To allow for more results, select the Use classic charts option in Global Preferences. By default, you can view a maximum of 99 results for classic charts. To increase the number of results that you can view, add the following property to the <code>console.properties</code> file and specify the desired value:</p> <pre>queryviewer.max.dashboard.chart.rows</pre> <p>For information about editing the <code>console.properties</code> file, see the ESM Administrator's Guide.</p>
NGS-28500	<p>Zoom functionality is not available for new event graphs.</p> <p>Workaround: To allow for zoom functionality on new event graphs, select the Use classic charts option in Global Preferences.</p>

ArcSight Manager

Issue	Description
NGS-27487	This patch resolves an issue where installation of Activate package bundles in environments with FIPS mode enabled sometimes failed.
NGS-28136	<p>Using a key size other than 2048 might impact performance.</p> <p>Workaround: Micro Focus recommends using a key size of 2048 when you generate certificates for the Manager, but you can specify a key size up to 4096. Increasing the key size will increase encryption strength, but might result in a decrease in performance because of increased CPU usage.</p>
NGS-28169	This patch resolves an issue where the Memory, Hostinfo, and Exceptions sections and information related to longest full garbage collection (GC) were missing from the HTML output that the <code>logfu</code> command generated.
NGS-28512	<p>When using ESM in distributed correlation mode, the default capacity of internal buffers that temporarily store incoming events might limit persistence throughput.</p> <p>Workaround: If the incoming event rate is greater than 25,000 events per second (EPS), add the following lines to the <code>server.properties</code> file, and then restart the ESM cluster:</p> <pre>queue.logger.pre-security-event-persistor.capacity=200000 queue.logger.start-of-flow.capacity=200000</pre> <p>For information about editing the <code>server.properties</code> file, see the ESM Administrator's Guide.</p>

Command Center

Issue	Description
NGS-28418	This patch resolves an issue where some fields within Case categories (for example, Ticket > Stage and Security Classification > Vulnerability) did not appear correctly in the legend in query viewers.
NGS-28655	This patch resolves an issue where Command Center did not display the country flag that was associated with country names and codes.

Connectors

Issue	Description
NGS-27651	<p>The Forwarding Connector log might contain the following exception when you configure Event Broker as a destination:</p> <pre>FATAL EXCEPTION: com.arcsight.common.config.w: An error occurred in configuration. Unable to find requested property 'transport.cefkafka.extra.prod.props'.</pre> <p>This exception does not impact the performance or functionality of the Forwarding Connector.</p>

CORR-Engine

Issue	Description
NGS-27096	<p>ESM generates errors when you use the Optimize Data feature with an active list and do not define any keys.</p> <p>Workaround: Deselect the Optimize Data feature. The Optimize Data feature for active lists is deprecated.</p>
NGS-27893	This patch resolves an issue where if you specified a "/" in the distinguished name for a user in Active Directory, the user could not log in to ESM.

Issue	Description
NGS-28027	<p>In a distributed cluster where large lists are present, upon cluster startup it might take some time for the lists to load and for events per second (EPS) to increase. ESM might generate a <code>ConcurrentModificationException</code> error in the logs.</p> <p>Workaround: If ESM generates a <code>ConcurrentModificationException</code> error, add the following property to the <code>server.properties</code> file, and then restart the cluster:</p> <pre>activelist.parallel.load.threshold=false</pre> <p>For information about editing the <code>server.properties</code> file, see the ESM Administrator's Guide.</p>
NGS-28062	<p>This patch resolves an issue where ESM triggered actions that were related to active lists when you replayed a rule, but failed to trigger other types of rule actions.</p>
NGS-28191	<p>Session list variables are not suitable for aggregation fields in rules. You might notice performance impacts because of increased database queries.</p> <p>Workaround: To avoid performance issues, if session list variables are not associated with the actions for a rule, remove them from the aggregation fields. If a rule does have session list variables associated with its actions, disable the rule.</p>
NGS-29051	<p>This patch resolves an issue where in distributed mode, ESM miscounted the audit events in data monitors.</p>

General

Issue	Description
NGS-28431	<p>This patch resolves an issue where ESM did not attach empty reports when it sent email notifications for empty reports.</p> <p>If you do not want to attach the empty reports, set the following properties in the <code>server.properties</code> file of the ArcSight Manager:</p> <ul style="list-style-type: none"> <code>report.scheduler.attach_empty_reports=false</code> <code>report.scheduler.notify_empty_reports=false</code> <p>For information about editing the <code>server.properties</code> file, see the ESM Administrator's Guide.</p>

Open Issues

The section provides information about open issues in this release.

Command Center

Issue	Description
NGS--28960	<p>If you attempt to view case metrics for more than 50,000 cases in the SOC Manager, Command Center does not display the metrics.</p> <p>If you attempt to view analyst metrics and the analyst has more than 5,000 cases, Command Center does not display the metrics.</p>
NGS-29055	<p>Field names are not available when configuring a filter for a new channel.</p> <p>Workaround: Refresh the page.</p>
NGS-28901	<p>Dashboard charts might not render properly.</p> <p>Workaround: Refresh the page.</p>

ArcSight Console

Issue	Description
NGS-28602	<p>The option that allows you to display a world map with country borders, a world map without country borders, or a custom map in the background is not enabled by default.</p> <p>Workaround: Select Edit > Preferences > Global Options, select the desired setting for the Geo Map Type global option, and then select Use classic charts.</p>

Correlation

Issue	Description
NGS-28849	<p>If a rule creates a large number of cases (500,000 or more), the persistor and embedded dcache might run out of memory.</p> <p>Workaround: Use the Manager Configuration Wizard to increase the Java heap memory size.</p> <p>For more information about using the wizard, see the ESM Administrator's Guide.</p>
NGS-28860	<p>In cases of network outages, if you modify a rule (for example, a filter, aggregation, or action) from the ArcSight Console, correlators and aggregators are no longer synchronized with the Manager and the Manager invalidates the rule.</p> <p>Workaround: Restart the cluster services and then run the <code>resvalidate</code> command with the <code>persist</code> option set to <code>true</code>.</p> <p>For information about the <code>resvalidate</code> command, see the ESM Administrator's Guide.</p>
NGS-28984	<p>When you make changes to an active list or a session list (for example, remove list entries), the changes might not be visible in the ArcSight Console until background persistence processing is complete.</p> <p>Workaround: Wait for the background persistence processing to complete. The processing usually takes less than one minute but might take several minutes in environments with lists that change frequently.</p>

Manager

Issue	Description
NGS-28789	<p>If you are running SNMP version 3 and the SNMP server is not available, a timeout issue in the SNMP library might cause events per second to drop.</p> <p>Workaround: Use SNMP version 1.</p>
NGS-28788	<p>You might receive an unknown error when you attempt to log in to ArcSight Command Center.</p> <p>Workaround: Create a new admin user and log in.</p>

Open and Closed Issues in Previous Releases

For information about open and closed issues for ESM 7.0 Patch 1, 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 7.0 Patch 2)

Just add your feedback to the email and click send.

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

We appreciate your feedback!