Micro Focus
ArcSight Management Center

Software Version: 2.9.6

Release Notes

Document Release Date: December, 2020
Software Release Date: December, 2020

MICRO FOCUS®

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

© Copyright 2013-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

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

About ArcSight Management Center

ArcSight Management Center (ArcMC), one of the Security Open Data Platform (SODP) family of products, is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective way.

ArcMC offers these key capabilities:

- **Management and Monitoring:** A single management interface to administer and monitor ArcSight managed nodes, such as: Transformation Hub, Loggers, Collectors, Connectors, Connector Appliances, and other ArcMC instances.
- **Connector Deployment:** Remotely deploy and manage connectors across your network.
- **SmartConnector Hosting:** For the hardware appliance, ArcMC hosts SmartConnectors.

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies
- Increased level of accuracy and reduction of errors in configuration of managed nodes
- Improves operational capabilities and lower total cost of ownership

What's New in this Release

This version of ArcMC includes the following new features and enhancements:

- Deployment and configuration of Transformation Hub in an Amazon Web Services (AWS) environment that leverages its cloud-native services and capabilities.
- Support for the latest SmartConnector release, v8.1.0. In addition to CEF and ESM_Binary formats, this release now supports emitting Avro-formatted event streams.
- ArcMC and Transformation Hub have been enhanced to enable routing of Avro streams and consumption and routing of Avro events forwarded from ESM or Logger.
- Windows Native Connector (WiNC) on a Connector Host Appliance (CHA) can now run in a Windows 2019 Server VM on Gen10 CHAs.
- New dashboard - A new list view dashboard shows host systems in an exception status (FATAL, CRITICAL, or WARNING). Pertinent information like the container and rule that was breached is displayed. It is periodically refreshed like other dashboards.
- New Device Export Option - Device export can now use recent and locally cached status data from the last refresh to generate the device status report .csv file. In prior releases, device export queried each device in real-time, causing long delays when there were hundreds or thousands of devices.

- When the new ArcMC_Instance_Name= property is configured, this instance name is shown in all pages to uniquely identify the ArcMC instance.
- The last refresh time is now shown in 24-hour military time.
- Platform component version updates have been certified on RHEL 8.2, CentOS 8.2 with updated releases of Azul Zulu Java runtime and Apache Tomcat. Component libraries include current vulnerability compliance, and ciphers are up-to-date.
- Miscellaneous bug fixes.

For more information about this release, review the following sections:

- "Fixed Issues" on page 14.
- "Open Issues" on page 17.

For detailed information about ArcMC features and functionality, refer to the ArcMC Administrator's Guide, and other documentation, available from the ArcSight Product Documentation Community.

Technical Requirements

For ArcSight Management Center

Server	For software form factor:
	• Red Hat Enterprise Linux (RHEL) 8.2, 8.1, 7.8, 7.7, 6.10. Additionally, for RHEL 7.x installation of software ArcMC: See *"Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x" on page 9*.
	• CentOS 8.2, 8.1, 7.8, 7.7, 6.10.
	For appliance upgrade: Red Hat Enterprise Linux 7.8, and 6.10.
Client System	• Windows 7, 8, 10
	• RHEL 6.10, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.1.
CPU	1 or 2 Intel Xeon Quad Core (or equivalent)
Memory	• 16 GB RAM
	• 80 GB Disk Space (for software form factor)
Supported Client Browsers	• Microsoft Edge (version current as of release date)
	• Firefox ESR (version current as of release date)
	• Google Chrome (version current as of release date)
Screen Resolution	Optimal screen resolution is 1920x1200
Hardware Models	For upgraded deployments, all models C660x and C670X running RHEL 7.8, as well as models C65XX running on RHEL 6.10.

For Managed ArcSight Products

Managed Node	Form Factor	Supported	Certified	Appliance Model
ArcMC	Software and Appliance	• 2.9.5 • 2.9.4 • 2.9.3.1 • 2.9.2 • 2.9.1 • 2.9.0	• 2.9.6	• C6700 • C6600 • C6500
SmartConnector	Software	• 8.0 • 7.15 • 7.14	• 8.1	
Collector	Software	• 8.0 • 7.15 • 7.14	• 8.1	
Logger	Software and Appliance	• 7.1 • 7.0.1 • 7.0	• 7.1.1	• L7700 • L7600 • L7500
Transformation Hub	Software	• 3.3 • 3.2	• 3.4	
ESM	Software	• 7.3 • 7.2 SP1 • 7.2	• 7.4	

Installer Files

The installation package is available for download from the ArcMC 2.9.6 Software Depot at https://entitlement.mfgs.microfocus.com. The installer files for ArcSight Management Center 2.9.6 are named as follows:

- **For Software ArcMC:** ArcSight-ArcMC-2.9.6.<build_number>.0.bin
- **Software installer for use remotely with the ArcMC Node Management as well as local upgrade:** arcmc-sw-<build_number>-remote.enc
- **For ArcMC Appliance (Upgrade Only):** arcmc-<build_number>.enc

- **ArcMC Agent Installer:** The ArcMC Agent installer for all appliance nodes, and all types of software nodes, is bundled with the ArcMC installer file. You may remotely install or upgrade the ArcMC Agent on a managed node directly from ArcMC, as follows:

- The installation of the ArcMC agent is performed when adding the nodes through Node Management (**Add Host** section). For more information refer to **Chapter 2: Software Installation / Installing the Arcsight Management Center Agent** in the ArcMC Adminstrator's Guide. For upgrading the agent on managed nodes check **Chapter 5: Managing Nodes / Updating (or Installing) the ArcMC Agent.**

- You can install or upgrade the ArcMC Agent remotely from a managing ArcMC on all managed appliance nodes (Logger Appliance, and ArcMC Appliance).

- You can install or upgrade the ArcMC agent for remotely managed software nodes which are ArcMC v2.2 and Logger v7.0 or later.

> **Note:** The ArcMC Agent cannot be upgraded or installed remotely on earlier versions of ArcMC and Logger, nor for any software Connector Appliance managed node. For these node types, the manual installer is required and named `ArcSight-ArcMCAgent-2.9.6.<build_number>.0.bin`.

ArcMC Appliance OS Upgrade Files

The OS Upgrade files are available for download from the ArcMC 2.9.6 Software Depot at https://entitlement.mfgs.microfocus.com. The OS upgrade files for ArcSight Management Center 2.9.6 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.10: (C650x appliances)** `osupgrade-arcmc-rhel610-<timestamp>.enc`

- **For Upgrade to RHEL 7.8: (C660x appliances)** `osupgrade-arcmc-rhel78-<timestamp>.enc.`

> **Note:** For OS upgrade files for a software ArcMC host, contact your host vendor.

Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x

Before installing or upgrading software ArcMC on Red Hat Enterprise Linux (RHEL) 7.X, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the logind.conf file for RHEL 7.X:

1. Navigate to the **/etc/systemd** directory, and open the **logind.conf** file for editing.

2. Find the **RemoveIPC** line. **RemoveIPC** should be active and set to *no.* (Remove the # sign if it is there, and change the yes to no if appropriate. The correct entry is: **RemoveIPC=no**).

3. Save the file.

4. From the **/etc/systemd** directory, enter the following command to restart the systemd-logind service and put the change into effect: `systemctl restart systemd-logind.service`

After you have modified this setting and met any other prerequisites, you are ready to install software ArcMC.

Upgrading ArcMC

Upgrade is supported from software ArcSight Management Center version 2.9.0 and 2.9.5 to software ArcSight Management Center 2.9.6. You should also upgrade any managed ArcMCs to version 2.9.6 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.9.6.

- **OS Upgrade:** Upgrade the operating system on your appliance or host to a supported OS version *before* upgrading the ArcMC version. OS support and required OS upgrade file names are listed under Technical Requirements.

  > **Note:** Because the latest OS includes important security updates, be sure to apply the OS upgrade even if you already upgraded the OS version to 6.10 or 7.8.

  For instructions on how to apply an appliance OS upgrade (either remotely or locally), see the section on Upgrading ArcMC in the ArcMC Administrator's Guide.

  > **Note:** For OS upgrade files for a software ArcMC host, contact your host's vendor.

These instructions are for upgrading software ArcMC using a wizard in GUI mode. You can also upgrade your ArcMC from the command line in console mode, and in silent mode. For those instructions, refer to the Installation chapter of the ArcMC Administrator's Guide.

Remote upgrade is another method if the target ArcMC is managed by another ArcMC using the Node Management upgrade feature.

> **Note:** As a recommendation, you should perform a backup of your current ArcSight Management Center configuration before upgrading to ArcMC 2.9.5. For more information see the **Managing Backups and Restores** section on the ArcMC Administrator's Guide.

To upgrade to ArcSight Management Center 2.9.6:

1. If you have previously configured SMTP for ArcMC, you must delete all SMTP configuration files before starting the upgrade. This step only applies if upgrading from ArcMC 2.8.1 or earlier.

a. Open the **Configuration Management** > **All Subscriber Configurations** page.

b. For all configurations of the type SMTP, click the **Name** link to open the configuration details. Make a note of the configuration. You will use this information to restore the SMTP configuration after the upgrade.

c. Then select the configuration and click **Delete**.

2. Copy the required upgrade files to a secure network location.

3. Run these commands from the directory where you copied the ArcSight Management Center files:

```
chmod u+x ArcSight-ArcMC-2.9.6.<build_number>.0.bin
./ArcSight-ArcMC-2.9.6.<build_number>.0.bin
```
The installation wizard starts. Review the dialog box, and then click **Continue**.

4. Follow the prompts to upgrade. For your installation directory, choose your original ArcSight Management Center installation directory.

5. If you run the ArcSight Management Center software installer as a root user, then you need to specify an existing non-root user and a port through which ArcSight Management Center users will connect. If any port other than 443 (the default HTTPS port) is specified, then users will need to enter the port number in the URL they use to access ArcSight Management Center. When prompted, enter the user name of the non-root user and the HTTPS port number, and then click **Next**.

6. Follow the prompts to complete product initialization.

7. If you run the installer as a root user, specify whether to run ArcSight Management Center as a system service or as a process.

> **Note:** Additionally, a few libraries are added using `ldconfig`. For a complete list of those libraries, see `/etc/ld.so.conf.d/arcsight_arcmc.conf` and `<install_dir>/current/arcsight/install/ldconfig.out.`

The upgrade is completed.

8. Click **Start ArcSight Management Now**, or click **Start ArcSight Management Center later**, and then click **Finish**.

9. If you deleted SMTP configurations files in "If you have previously configured SMTP for ArcMC, you must delete all SMTP configuration files before starting the upgrade. This step only applies if upgrading from ArcMC 2.8.1 or earlier. " on the previous page, you can now open the **Configuration Management > All Subscriber Configurations** page and restore your SMTP configurations from your notes.

Upgrading the ArcMC Agent

You should also upgrade the ArcMC Agent on all managed nodes that require the Agent for communication with ArcMC. For instructions on upgrading the ArcMC Agent on managed nodes, see the ArcMC Administrator's Guide.

Fixed Issues

The following issues are fixed in this release.

Issue	Description
ARCMC-16960	Connectors were not upgrading when performing a bulk upgrade.
ARCMC-16809	Transformation Hub node managed by ArcMC would become unreachable after upgrading to Transformation Hub 3.3.
ARCMC-16724	Some Logger configurations were returning error messages instead of importing successfully.
ARCMC-16638	The logger configurations Logger SmartMessage Receiver or Configuration Backup or Logger Transport Receiver could not be imported or pushed to Loggers 7.1.0
ARCMC-16573	After upgrading a software Logger from ArcMC, the ArcMC system displayed an error "Upgrade failed - Failed to bring up all processes successfully."
ARCMC-16472	Device export could take up-to several hours to be completed if the customer's ARCMC has more than 3 digit devices.
ARCMC-16151	ArcMC could not connect to Collector 7.14 and 7.15 after enabling FIPS mode on Collectors.
ARCMC-11220	On a freshly imaged ARI for ArcMC 2.60 or 2.70, when you restarted the web process for the first time, you could only access the System & Admin page and not to the navigational menus.
ARCMC-11140	When choosing "Export" from the Node Management menu while viewing a feature other than Node Management, the page remained blank or showed a spinner indefinitely, although the export succeeded.

Known Issues

ArcMC is known to have the following limitations.

Issue	Description

ARCMC-17065	When upgrading ArcMC 2.9.5 to 2.9.6, please verify the following file exists on the file system before performing the upgrade:
	
	For software ArcMC:
	`find $INSTALL_FOLDER/arcmc/data/postgres_11_4_upgrade_completed`
	For appliance ArcMC:
	`find /opt/arcsight/userdata/pgsqlbk/postgres_11_4_upgrade_completed`
	If this file does not exist, follow the procedure below (only for upgrading from 2.9.5 to 2.9.6)
	
	For software ArcMC:
	
	Check if the PostgreSQL version is 11.4:
	`cat $INSTALL_FOLDER/arcmc/data/pgsql/PG_VERSION`
	If the output is "11", execute the following commands:
	`cd $INSTALL_FOLDER/arcmc/data/`
	`touch postgres_11_4_upgrade_completed`
	For appliance ArcMC:
	
	Check if the PostgreSQL version is 11.4:
	`cat /opt/arcsight/userdata/pgsql/PG_VERSION`
	If the output is "11", execute the following commands:
	`cd /opt/arcsight/userdata/pgsqlbk/`
	`touch postgres_11_4_upgrade_completed`

ARCMC-17041	Issue: When creating or editing a route rule, the drop down menu to select the conditions does not work on Firefox. Workaround: Use a different browser.
ARCMC-16757	Issue: When performing a remote upgrade of Loggers 7.0 .1 or earlier, to 7.1.0 or later, the process may appear as if it timed-out on ArcMC. However, the upgrade process will continue as expected on Logger. To increase the timeout add the **node.upgrade.thread.timout= 10800** (unit value in seconds) property to ArcMC's `logger.properties` file before upgrading. For more information regarding this procedure, please see the section *Modifying logger.properties* in the ArcMC Administrator's Guide.

Issue	Description
ARCMC-16723	Issue: The Logger monitoring page is not displaying the Logger 7.1.0 stats. Workaround: None available at this time.
ARCMC-16716	Issue: Upgrading to ArcMC 2.9.5 is not supported on G8 appliances.
ARCMC-16638	Issue: The logger configurations Logger SmartMessage Receiver, Configuration Backup, and Logger Transport Receiver can't be imported from nor pushed to Loggers 7.1.0. Workaround: Manually configure Logger SmartMessage Receiver, Configuration Backup, and Logger Transport Receiver.
ARCMC-14051	Issue: ArcMC is showing run-time parameters page instead of connector parameters. Workaround: Log off and log back in to reset behavior or click another tab at the top, i.e. configuration etc., then go back to node management.

Open Issues

This release contains the following open issues.

Issue	Description
ARCMC-17022	Issue: If one Transformation Hub is added and then removed from the ArcMC, the information in /etc/hosts remains there. If a new Transformation Hub is added when the user tries the 1-Click Collector it will fail. Workaround: Before adding the information for the new Transformation Hub in the /etc/hosts users need to remove the information from the previous Transformation Hub.

ARCMC-16923	Issue:
	
	For ArcMC 2.9.6 fresh install, the parameters on **postgresql.conf** for timezone are not set during installation.
	
	Workaround:
	
	Modify the /opt/arcmc/data/pgsql/postgresql.conf file as shown below:
	
	`max_connections = 500`
	
	`shared_buffers = $PGBUFFER`
	
	`autovacuum = off`
	
	`datestyle = 'iso, mdy'`
	
	`lc_messages = 'en_US.UTF-8'`
	
	`lc_monetary = 'en_US.UTF-8'`
	
	`lc_numeric = 'en_US.UTF-8'`
	
	`lc_time = 'en_US.UTF-8'`
	
	`default_text_search_config = 'pg_catalog.english'`
	
	`log_line_prefix = '%m ' #Custom log format`
	
	`timezone = LOCAL_TIME_ZONE (e.g. America/Los_Angeles)`
	
	`log_timezone = LOCAL_TIME_ZONE (e.g. America/Los_Angeles)`

Issue	Description
ARCMC-16960	Issue: Connectors are not upgrading when performing a bulk upgrade. Workaround: Before performing a bulk upgrade of Smart Connectors on a given Linux server (any server including the ArcMC appliance), please install the appropriate rng-tools version for the flavor/version of the Linux OS. However, this is not required if the bulk upgrade involves only one Smart Connector per Linux server or on Windows server.
ARCMC-16961	Issue: Instant Deployment of Collectors using a non-root user of the remote machine where collector will be installed fails at the last step. Workaround: None available at this time.
ARCMC-16954	Issue: The Host Status Exceptions page is not displaying the Transformation Hub rules. Workaround: None available at this time.
ARCMC-16951	Issue: If there are connectors installed in the path /opt/arcsight/connector*/, the ArcMC upgrade will fail. Workaround: Move the connectors to another location during upgrade.
ARCMC-16933	Issue: When deploying a CTH the destination topic drop-down will not be populated the first time the panel is opened on a browser, once the information is cached on the browser the panel will be populated. Workaround: Open and close the panel for the destination topic drop-down to be populated.
ARCMC-16737	Issue: When attempting to Remove Transformation Hub from ArcMC, it results in a blank message window, and the Transformation Hub is not removed from the ArcMC. Workaround: Please contact the Support team to address this issue.

Issue	Description
ARCMC-16682	Issue: ArcMC stops Logger Appliance upgrades due to a 40 minutes timeout Workaround: Increment the timeout variable in ArcMC before the Logger upgrade: 1. cd /$ARCMC_HOME/userdata/arcmc 2. As <no root user>, create the logger.properties file if it does not exist. 3. Add a new entry **node.upgrade.thread.timout=10800** in logger.properties 3.1. The unit in seconds. 10800sec = 3hours 4. chown <no root user>:<no root user> logger.properties 5. chmod 660 logger.properties 6. Restart ArcMC
ARCMC-16514	Issue: 'Unknown' consumer type with internal cluster IP address is seen intermittently on Topology and Deployment views. The problem appears to be caused by the timing of docker and firewall. Workaround: Rebooting all hosts in the cluster may solve the problem.
ARCMC-15844	Issue: ArcMC does not support the following logical operators for Transformation Hub rule creation: NOT DOESNOTCONTAIN Workaround: Use the **NOT** and **contains** operators to support the **DOESNOTCONTAIN** operator.
ARCMC-13790	Issue: On the Topology and Deployment view, the incorrect Alternate location icon is shown for Collectors. On the Deployment view the Alternate location icon is not shown on the legend. Workaround: None available at this time.

Issue	Description
ARCMC-13332	Issue: Network IP address is not saved into the system. Workaround: Manually perform the "edit - save" function to save the network IP address before restoring.
ARCMC-12847	Issue: After SecureData FPE encryption is enabled, it should not be disabled. However, ArcMC permits the user to disable it. Doing so will leave the event output in an inconsistent state. Workaround: Do not disable SecureData FPE encryption once it has been enabled.
ARCMC-10478	Issue: After a product type ages out (Device Age-Out) there is no way for the user to get that product type back. If Device Tracking is disabled for a device product and the device ages out, then there is no way to revert to enable tracking for that device product. Workaround: None available at this time.

Security Fixes

The following security fixes were implemented in this release.

Description	CVE
* Code Injection	CVE-2020-11851
** Stored XSS	CVE-2020-25835

* Special thanks to Security Researcher Chinghz Saferli, for responsibly disclosing this vulnerability.

** Special thanks to Nikita Loginov from Gazinformservice, for responsibly disclosing this vulnerability.

Documentation Errata

Document Affected: ArcMC Online Help

- In the section *Deployment View*, the **Note** at the end of the *Prerequisites for Instant Connector Deployment* page is displaying an invalid link to download the specified rpm package. Please refer to ArcMC's Administrator's Guide, Chapter 4 > Page 74 for the correct information.

- In the section *Enabling SecureData Encryption on Managed Connectors*, the **Note** at the end of the *Prerequisites for Addition of SecureData Client to Multiple Containers* page is displaying an invalid link to download the specified rpm package. Please refer to ArcMC's Administrator's Guide, Chapter 7 > Page 233 for the correct information.

- In the section *Enabling SNMP on Software ArcMC*, the **Note** under step 9 in *To enable SNMP notifications on a software host* is missing from the online help. Please refer to ArcMC's Administrator's Guide, Chapter 4 > Page 70 for the correct information.

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 (ArcSight Management Center 2.9.6)

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!