Micro Focus
ArcSight Management Center

Software Version: 2.9.5

Release Notes

Document Release Date: September, 2020
Software Release Date: July, 2020

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

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:

- Support for the latest Connector release, v8.0.0.
- Windows Native Connector (WiNC) on a Connector Host Appliance (CHA) can now run in a Windows 2019 Server VM on Gen9 CHAs. For more information, please refer to the SmartConnector Microsoft Windows Event Log Native on CHA documentation.
- Event routing and filtering in Transformation Hub for events transformed from CEF to Avro format and consumed by ESM, Interset, and Investigate. These events may now be stored in a common high-performance Vertica database shared by all ArcSight products. If you want more in depth information regarding this feature, see the Transformation Hub Documentation.
- Configuration for the new AWS Cloud S3 SmartConnector
- Configuration of Transformation Hub processing in Microsoft Azure environment that leverages Azure services and capabilities.
- Platform component version updates have been certified on RHEL 7.8, CentOS 7.8 (RHEL/CentOS 8.1 was already supported in 2.9.4), with updated releases of Azul Zulu Java runtime, PostgreSQL and Tomcat. Component libraries include current vulnerability compliance, and ciphers are up-to-date.

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

- "Fixed Issues" on page 14.
- "Open Issues" on page 16.

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) 8.1, 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 8.1, 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.

For Managed ArcSight Products

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

Installer Files

The installation package is available for download from the ArcMC 2.9.5 Software Depot at https://entitlement.mfgs.microfocus.com. The installer files for ArcSight Management Center 2.9.5 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.9.5.<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-2.9.5.<build_number>.0.bin`.

ArcMC Appliance OS Upgrade Files

The OS Upgrade files are available for download from the ArcMC 2.9.5 Software Depot at https://entitlement.mfgs.microfocus.com. The OS upgrade files for ArcSight Management Center 2.9.5 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 2.9.4 to software ArcSight Management Center 2.9.5. You should also upgrade any managed ArcMCs to version 2.9.5 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.9.5.

- **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 2.9.5:

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-2.9.5.<build_number>.0.bin
./ArcSight-ArcMC-2.9.5.<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-16300	ArcMC Restore failed when database size was too large.
ARCMC-16284	Export button was not working on Microsoft Edge and Internet Explorer.
ARCMC-16282	Import hosts was not working on Microsoft Edge and Internet Explorer
ARCMC-16161	Unable to add more than 11 ArcSight Logger SmartMessage Pool (encrypted) destination through ArcMC.
ARCMC-16125	Azure Event Hub destination option not available for ArcMC Appliance's local containers
ARCMC-16105	Remove the static key ciphers.
ARCMC-15651	`snmpget` command was not working in software ArcMC.
ARCMC-14963	ArcMC UI "Configure Memory Settings" container command did not reflect the correct current memory number.
ARCMC-2129	When a Connector is managed by two ArcMCs and the two ArcMCs had different Content AUP's uploaded, multiple copies of the same Content AUP file were created in the user/agent/aup directory. This caused large appliance backup files to accumulate, occupying disk space.

Known Issues

ArcMC is known to have the following limitations.

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.
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-16573	Issue: After upgrading a software Logger from ArcMC, the ArcMC system displays an *"Upgrade failed - Failed to bring up all processes successfully"* error. The Logger is upgraded successfully and all processes are running except for the ArcMC Agent (arcmagent) process. Workaround: Update the ArcMC Agent from ArcMC. 1- Go to Node Management > Hosts tab 2- Select the Logger that was previously upgraded 3- Click Update Agent
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 firewalld. Workaround: Rebooting all hosts in the cluster may solve the problem.
ARCMC-16473	Issue: Azure CTH Deployment job will fail in ArcMC if users don't properly configure Azure load balancer and inbound port rules. Workaround: 1- Open `logger.properties` file for editing 2- Update the `configuration.cth.start.port` to 32101, the `configuration.cth.end.port` to 321501 and save your changes. 3- Restart the web process `ARCMC_HOME/bin/arcmcd restart web`
ARCMC-16472	Issue: Device export can take up-to several hours to be completed if the customer's ARCMC has more than 3 digit devices. Workaround: None available at this time.

Issue	Description
ARCMC-16151	Issue: ArcMC cannot connect to Collector 7.14 and 7.15 after enabling FIPS mode on Collectors. Workaround: None available at this time.
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.
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.

Issue	Description
ARCMC-11220	Issue: On a freshly imaged ARI for ArcMC 2.60 or 2.70, when you restart the web process for the first time, you will have access to only System & Admin page and no access to navigational menus. Workaround: If you have access only to System Admin page, restart the apps process on Process Status page. Once the apps process restarts and is running, restart the web process. You should now have access to all menus.
ARCMC-11140	Issue: When choosing "Export" from the Node Management menu while viewing a feature other than Node Management, the page may remain blank or show a spinner indefinitely, although the export will succeed. Workaround: Select Node Management from the menu first, and after the page has loaded, click Export.
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.

PSRT Case	Description	CVE
38984	Denial of Service	CVE-2020-11848

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

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 2.9.5)

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!