
Micro Focus

ArcSight Management Center

Software Version: 2.9.2

Release Notes

Document Release Date: July, 2019

Software Release Date: July, 2019



Legal Notices

Copyright Notice

© Copyright 2013-2019 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.

US. 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 US 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://software.support.softwaregrp.com/support-contact-information
Support Web Site	https://software.support.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

About ArcSight Management Center	4
What's New in this Release	4
Technical Requirements	5
For ArcSight Management Center	5
For Managed ArcSight Products	6
Installer Files	6
ArcMC Appliance OS Upgrade Files	7
Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x	7
Upgrading ArcMC	8
Upgrade Prerequisites	8
Fixed Issues	10
Open Issues	12
Send Documentation Feedback	15

About ArcSight Management Center

ArcSight Management Center (ArcMC), one of the ArcSight Data Platform (ADP) 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:** Deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Transformation Hub, Loggers, Collectors, Connectors, Connector Appliances, and other ArcMCs.
- **Connector Deployment:** Remotely deploy and manage connectors across your network.
- **SmartConnector Hosting:** For the hardware appliance, as a platform to host and 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
- Reduction in operational expenses

What's New in this Release

This version of ArcMC includes the following features and enhancements:

- **Bulk emergency restore:** Users can perform emergency restore of multiple local containers at once. This feature also provides a way to migrate local containers from 32 bit to 64 bit . The existing connector configuration will be preserved after the migration process.
- **Host Tab Feature Migration:** Functionalities under **Node Management > Hosts tab** can now be found in **Configuration Management > Bulk operations > Hosts tab**.

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

- ["Fixed Issues" on page 10.](#)
- ["Open Issues" on page 12.](#)

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	<p>For software form factor:</p> <ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 6.10, 7.3, 7.4, 7.5, 7.6. Additionally, for RHEL 7.x installation of software ArcMC: See "Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x" on page 7.• CentOS 6.9, 6.10, 7.4, 7.5, 7.6. <p>For appliance upgrade: Red Hat Enterprise Linux 6.10, 7.6.</p>
Client System	<ul style="list-style-type: none">• Windows 7, 8, 10• RHEL 6.9, 7.3, 7.4, 7.5.
CPU	1 or 2 Intel Xeon Quad Core (or equivalent)
Memory	<ul style="list-style-type: none">• 16 GB RAM• 80 GB Disk Space (for software form factor)
Supported Client Browsers	<ul style="list-style-type: none">• Internet Explorer 11• 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 C550x and C650x running RHEL 6.10; all models C660x running RHEL 7.6.

For Managed ArcSight Products

Managed Product	Software Form Factor	Hardware (Appliance)	ArcMC Agent Version Required
SmartConnector	v6.0.3 or later. Applies to software connectors running on ArcMC Appliance, Connector Appliance, Logger (L3XXX), or separate server.	N/A	ArcMC Agent is not required.
Logger	v6.2 or later.	v6.1 or later on models LX50X and LX60X	v2.71, v2.9.2
ArcMC	v2.2 or later.	v2.1 or later on models C650X and C660X.	v2.71, v2.9.2
Transformation Hub	v3.0 or later.	N/A	ArcMC Agent is not required
Collector	v7.70 or later.	N/A	ArcMC Agent is not required

Installer Files

The installation package is available for download from the ArcMC 2.9.2 Software Depot at <https://entitlement.mfgs.microfocus.com>. The installer files for ArcSight Management Center 2.9.2 are named as follows:

- **For Software ArcMC:** ArcSight-ArcMC-2.9.2.<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 Administrator'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 v2.1 and Logger v6.0 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-2.9.2.<build number>.0.bin**.

ArcMC Appliance OS Upgrade Files

The OS Upgrade files are available for download from the ArcMC 2.92 Software Depot at <https://entitlement.mfgs.microfocus.com>. The OS upgrade files for ArcSight Management Center 2.9.2 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.10: (C650x appliances)** `osupgrade-arcmc-rhel610-<timestamp>.enc`
- **For Upgrade to RHEL 7.6: (C660x appliances)** `osupgrade-arcmc-rhel76-<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 to software ArcSight Management Center 2.9.2. You should also upgrade any managed ArcMCs to version 2.9.2 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.9.2.

- **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 7.6.

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.

To upgrade to ArcSight Management Center 2.9.2:

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-2.9.2.<build number>.0.bin
```


`./ArcSight-ArcMC-2.9.2.<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-15443	When creating long topic routes in Configuration management > Transformation Hub users were receiving an error. This is now fixed in ArcMC 2.92.
ARCMC-15423	ArcMC SW ArcMC and Logger remote upgrade function fixes upgrade-from version validation check in ArcMC 2.92 release.
ARCMC-15392	Users were unable to change remote container credentials in bulk, if the Connector credentials were different. This is now fixed in ArcMC 2.92.
ARCMC-15386	Required packages to successfully start Logger Linux installation as Cloud Linux images (AWS EC2 and Azure VM images) (RH 7.5 and CentOS 7.5) have been included.
ARCMC-15282	When customer selected Device Type for a Device Product containing the "/" character, an "Internal Server Error" error message was displayed. This is now fixed in ArcMC 2.92.
ARCMC-15271	Monitor and breach data purged in ArcMC 2.90 was failing. This is no longer happening.
ARCMC-15266	When a rules file was imported into the system without all the required property fields for each rule, the system would throw a 500 error and the page won't load the contents again until a new file is imported with all the necessary fields. Now the error message has been updated to indicate a list of mandatory properties.
ARCMC-15218	Custom rules were not getting parsed on Connector event 'name' field. This is now fixed in ArcMC 2.92.
ARCMC-15209	<p>For customers concerned about receiving notification (email/snmp/alert) alert on "device inactive" event, add the following property on logger.properties to disable the alert.</p> <p>Add the entry in \$ARCMC_USERDATA_FOLDER/arcmc/logger.properties if you want to disable "EMAIL and/or SNMP and/or and/or AUDIT" notification</p> <pre>device.inactive.email.notification.enabled=false device.inactive.snmp.notification.enabled=false device.inactive.audit.notification.enabled=false</pre>
ARCMC-15206	Pushing a user from ArcMC to logger v6.7 with imported permissions group no longer throws error "500 Internal Server".

Issue	Description
ARCMC-15180	We implemented the Monit version 5.25.3. This version solved the issue when the aps and postgres process don't stop. We implemented the changes on APE. Also, added additional configuration into the monitrc file to certify the correct functionality.
ARCMC-14580	The NOT operator is now supported for creating rules from ArcMC to Event Broker. DOESNOTCONTAIN can be achieved by using NOT and CONTAINS operator.
ARCMC-13720	When Transformation Hub goes to OutOfMemory state, ArcMC lost connection with the Transformation Hub and its status was displayed as 'Down' in ArcMC. This is no longer happening.
ARCMC-13719	The deployment or redeployment of a CTH no longer fails.
ARCMC-13321	If Collector certificates fails to download, the host with connectors will not fail to be added as a host in ArcMC.

Open Issues

This release contains the following open issues.

Issue	Description
ARCMC-15276	<p>Issue:</p> <p>When installing a Windows 2012/2016 Collector to ArcMC 2.9.2.10506.0 using instant deployment feature, it is installed correctly in the VM, however the collector is not visible in deployment or topology view. The status of the Collector shows complete in the job manager section.</p> <p>Workaround:</p> <p>Add the Collector manually through the Add host feature.</p>
ARCMC-15180	<p>Issue:</p> <p>The monit log shows that APS and postgresql restart after stopped by monit stop all.</p> <p>Workaround:</p> <p>After an upgrade, it is recommended to wait 15 minutes before executing the command monit stop all. If the users cannot wait the 15 minutes, they can execute the command monit stop all, and check if all the processes have stopped by using the command monit summary. In case, some processes do not stop after some time, users can run the command monit stop all again, this will completely stop the processes. They can verify by running the command monit summary.</p>
ARCMC-14051	<p>Issue:</p> <p>ArcMC is showing run-time parameters page instead of connector parameters.</p> <p>Workaround:</p> <p>None available at this time.</p>
ARCMC-13724	<p>Issue:</p> <p>In some cases, a collector will not be added as a managed node if deployed on an already existing host by using an IP address.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Delete host added with its IP Address.2. Add the same host as Collector with its FQDN.3. Scan the host for Connectors.
ARCMC-13626	<p>Issue:</p> <p>If a connector or collector deployment job is submitted without DNS configuration, the job will fail and Job Manager will not enable a retry.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Configure the necessary DNS settings or make sure that the remote VM is resolvable by ArcMC.2. Start a new job from the Deployment view.

Issue	Description
ARCMC-12926	<p>Issue:</p> <p>Remote Instant Connector/Collector Deployment from an ArcMC running RHEL/CentOS 6.9 to a remote Windows machine is not supported.</p> <p>Workaround:</p> <p>None available at this time.</p>
ARCMC-12861	<p>Issue:</p> <p>When Collector metrics are shown, the restart count is always 0.</p> <p>Workaround:</p> <p>None available at this time.</p>
ARCMC-12847	<p>Issue:</p> <p>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.</p> <p>Workaround:</p> <p>Do not disable SecureData FPE encryption once it has been enabled.</p>
ARCMC-12599	<p>Issue:</p> <p>In Internet Explorer 11, the Add button for Connectors and Collectors is disabled.</p> <p>Workaround:</p> <p>To add a Connector or Collector, use the Topology view, or view the page in a different browser.</p>
ARCMC-12282	<p>Issue:</p> <p>In Internet Explorer 11 or Edge, the Topology drill down view can freeze the application.</p> <p>Workaround:</p> <p>Use the latest supported versions of Chrome or Firefox.</p>
ARCMC-11220	<p>Issue:</p> <p>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.</p> <p>Workaround:</p> <p>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.</p>

Issue	Description
ARCMC-11140	<p>Issue:</p> <p>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.</p> <p>Workaround:</p> <p>To avoid this, choose the "Node Management" menu option first, and after the page has loaded, choose "Export".</p>
ARCMC-10478	<p>Issue:</p> <p>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.</p> <p>Workaround:</p> <p>None available at this time.</p>
ARCMC-2129	<p>Issue:</p> <p>When a Connector is managed by two ArcMCs and the two ArcMCs have different Content AUP's uploaded, multiple copies of the same Content AUP file are created in the user/agent/aup directory. This may cause large appliance backup files to accumulate, occupying disk space.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Manage the Connector from one ArcMC only OR have the Content AUP version uploaded on both ArcMCs. 2. Manually delete the backup files that are not required.

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 2.9.2)

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!