Micro Focus
ArcSight Management Center

Software Version: 2.81

Release Notes

Document Release Date: June 29, 2018
Software Release Date: June 2018

MICRO FOCUS®

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 2013-2018 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

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 Event Broker, Loggers, 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:

- **Secure Authenticated SMTP:** ArcMC can now send emails using a secured authenticated SMTP server
- **Clone Deployment Templates:** You can now copy values from an existing deployment template
- **Device Rules:** Ability to create, edit, and delete a device rule
- **Devices have Severity associated with them instead of Status:** Up is equivalent to "HEALTHY" and Down to "FATAL"
- **Sunburst Chart and corresponding breakdown table:** Is enhanced to show the severity instead of status
- **Support for three types of Acknowledgment modes for Connector in Event Broker (CEB)**
- **Support for 50 CEBs for Event Broker 2.21**

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

- "Fixed Issues" on page 12.
- "Open Issues" on page 14.

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) 6.9, 7.3, 7.4. Additionally, for RHEL7.x installation of software ArcMC: See *"Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x" on page 8*. • CentOS 6.9, 7.3, 7.4 For appliance upgrade: Red Hat Enterprise Linux 6.9, 7.3, 7.4
Client System	• Windows 7, 8, 10 • MacOS 10.8 or later • RHEL 6.9, 7.3, 7.4
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	• 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 6.9; all models C660x running RHEL 7.3 or 7.4.

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, v6.2 P1, v6.3, v6.3.1, v6.4, v6.41, v6.50, v6.51, v6.60 v6.61,	v6.1, v6.1 P1, v6.2, v6.2 P1, v6.3, v6.3.1, v6.4, v6.41, v6.50, v6.51, v6.60, on models LX50X and LX60X	v2.71
ArcMC	v2.2, v2.2 P1, v2.5, v2.5.1, v2.6, v2.61 v2.70, v2.71, v2.80, v2.81,	v2.1, v2.2, v2.2 P1, v2.5, v2.5.1, v2.6, 2.61, v2.7.0, v2.71, v2.80 on models C650X and C660X.	v2.71
Connector Appliance	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX400 or CX500	v2.71
Event Broker	v2.0, v2.01, v2.10, v2.20	N/A	ArcMC Agent is not required
Collector	v7.70, v7.80	N/A	ArcMC Agent is not required

Installer Files

Available from the HPE download site, the installer files for ArcSight Management Center 2.81 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.81.<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 for some 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:

- You can install or upgrade the ArcMC Agent remotely from a managing ArcMC on all managed appliance nodes (Logger Appliance, ArcMC Appliance, and Connector Appliance hardware form factor).
- You can install or upgrade the ArcMC agent for remotely managed software nodes which are ArcMC v2.1 and Logger v6.0 or later.

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-2.81.<build number>.0.bin`.

ArcMC Appliance OS Upgrade Files

Available from the HPE download site, the OS upgrade files for ArcSight Management Center 2.81 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.9: (C650x appliances)** `osupgrade-arcmc-rhel69-<timestamp>.enc`
- **For Upgrade to RHEL 7.4: (C660x appliances)** `osupgrade-arcmc-rhel74-<timestamp>.enc`.

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 2.80 to software ArcSight Management Center 2.81. You should also upgrade any managed ArcMCs to version 2.81 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.81.

- **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 6.9 or 7.4.

  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 2.81:

1. Copy the required upgrade files to a secure network location.
2. Run these commands from the directory where you copied the ArcSight Management Center files:

   ```
   chmod u+x ArcSight-ArcMC-2.81.<build number>.0.bin

   ./ArcSight-ArcMC-2.81.<build number>.0.bin
   ```

   The installation wizard starts. Review the dialog box, and then click **Continue**.

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

4. 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**.

5. Follow the prompts to complete product initialization.

6. 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.

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

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-14317	During a connector configuration push, the ArcMC upgrade would fail. This is no longer the case.
ARCMC-14314	For the ArcMC 2.8 appliance, the SNMPV3 feature does not work. This is no longer the case.
ARCMC-14313	The License Usage Chart was missing from the Administrator's Guide. This is no longer the case.
ARCMC-14059	The FTP link was not working on the ArcMC appliance, but this is no longer the case.
ARCMC-14041	The management of Event Broker routes does not allow for more than nine conditions. This is no longer the case.
ARCMC-13908	When using the One-Click feature to add a collector in Windows Server 2016, the collector will not appear as a manage node in ArcMC 2.8.0.2110. This is no longer the case.
ARCMC-13866	In the Node Management section, clicking the Location hyperlink when the left hand side tree is collapsed had no affect. This is no longer the case.
ARCMC-13865	On the Connector Summary page, refresh failed when the left side navigation tree was in the collapsed state. This is no longer the case.
ARCMC-13847	After deleting the Smart Connector for Microsoft Windows Event Log connector from the local container, you were not able to re-configure the local container. This is no longer the case.
ARCMC-13792	The Voltage client installation would fail for local containers. This is no longer the case.
ARCMC-13742	When trying to import rules, you would get the error: "Rule upload failed. Error: Cannot access the uploaded file: Upload Failed". This is no longer the case.
ARCMC-13739	In some scenarios when the deployment failed, ArcMC still tried to add the deployment as managed node. This is no longer the case.
ARCMC-13688	ArcMC cannot push a new user to Logger if the password policy is enforced. This is no longer the case.
ARCMC-13510	If you provided a passphrase of more than eight characters when configuring SNMP settings, audit events in the form of SNMP traps would not be sent. This is no longer the case.
ARCMC-13509	List of commands ArcMC runs when installing an Instant Connector.

Issue	Description
ARCMC-13501	ArcMC now supports Java 1.8.0.161.
ARCMC-13389	There are now `bulk-license-installer.zip` instructions in the ArcMC Administrator's Guide for using ArcMC to manage other products.
ARCMC-13095	The Release Notes document now has sections for Appliance OS Upgrade and for Appliance Upgrade.
ARCMC-13045	When upgrading ArcMC, duplicate default Monitoring Rules are no longer created.
ARCMC-12738	You can now add an email address for a user with a hyphen in domain name.
ARCMC-12128	ArcMC is now able to push a user to Logger.
ARCMC-12066	The CHA/ArcMC appliance now supports Smart Connectors.
ARCMC-10741	ArcMc can now push a new user to Logger when the password policy is enforced.
ARCMC-59	ConnApp 5.1 now displays the connector version at the "host" level of the Configuration tab.
ARCMC-7	There is now the ability to edit the `syslog.properties` file from the ArcMC user interface (Diagnostic tool).
ARCMC-6	You can now select the columns/fields for export to CSV and PDF files.

Open Issues

This release contains the following open issues.

Issue	Description
ARCMC-14380	Issue: Change the pullMetricData thread timeout as configurable property. Workaround: None.
ARCMC-14356	Issue: The 50 CEB and cert information in the online help are incorrect. Workaround: Please see the Administrator's Guide on Protect 724.
ARCMC-14311	Issue: When a new certificate is uploaded, the previously uploaded certificate is not deleted from the truststore. Workaround: Delete the previously added certificate from the truststore from command line and restart web.
ARCMC-13812	Issue: In some cases, attempting to deploy connectors with Instant Connector Deployment to a Windows host will produce a winrm or credssp failure, and connector deployment will fail. Workaround: None available at this time.
ARCMC-13790	Issue: In the Event Broker drill down view, the Collectors do not appear in different location displayed on this page as the event source for the CEBs on the Event Broker. Workaround: None.

Issue	Description
ARCMC-13740	Issue: When viewing a Collector container, the \Add\ button is incorrectly enabled. Attempting to add a collector using this button will fail and not add any collector on the host. Workaround: Use the Instant Deployment feature to deploy a collector on the host. Workaround: None.
ARCMC-13724	Issue: 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. Workaround: 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-13720	Issue: When Event Broker goes to OutOfMemory state, ArcMC loses connection with the Event Broker and its status is displayed as 'Down' in ArcMC. Workaround: Redeploy Event Broker. Once Event Broker is up and running, add the ArcMC details and certificate back in the Installer UI. Then ArcMC can manage the Event Broker successfully.
ARCMC-13719	Issue: The deployment or redeployment of a CEB can fail. Workaround: Complete the following to deploy or redeploy: 1. Login to the Installer. 2. Undeploy the Event Broker. 3. Redeploy the Event Broker. 4. Add ArcMC configurations to Event Broker. 5. The ArcMC user can now deploy or redeploy the CEB.

Issue	Description
ARCMC-13698	Issue: The retry option does not work for the SecureData client install. Workaround: 1. Fix the reason for the failure. 2. Open Manage Collector/Connector > Container. 3. Click **Properties** and run the install again.
ARCMC-13626	Issue: If a connector or collector deployment job is submitted without DNS configuration, the job will fail and Job Manager will not enable a retry. Workaround: 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.
ARCMC-13321	Issue: If a collector certificate fails to download, a host with connectors will also fail to be added as a host in ArcMC. Workaround: Manually add the host with just the Connector details (port) through "Add host".
ARCMC-13146	Issue: When performing a bulk delete of hosts, job processing may appear stuck but the job itself is completed. Workaround: None.
ARCMC-12926	Issue: Remote Instant Connector/Collector Deployment from an ArcMC running RHEL/CentOS 6.9 to a remote Windows machine is not supported. Workaround: None.
ARCMC-12861	Issue: When Collector metrics are shown, the restart count is always 0. Workaround: None.

Issue	Description
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. Warning: Do not disable SecureData FPE encryption once it has been enabled.
ARCMC-12785	Issue: A CEB name with special characters will show as agent name on the Connectors tab. Workaround: Avoid using special characters when naming CEBs.
ARCMC-12599	Issue: In Internet Explorer 11, the Add button for Connectors and Collectors is disabled. Workaround: To add a Connector or Collector, use the Topology view, or view the page in a different browser.
ARCMC-12282	Issue: In Internet Explorer 11 or Edge, the Topology drill down view can freeze the application. Workaround: Use the latest supported versions of Chrome or Firefox.
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-11219	Issue: In some cases, a Kafka timeout causes an intermittent topic bootstrap failure. Because of this, route creation in ArcMC may fail. Workaround: Restart webservices on the Event Broker master node.

Issue	Description
ARCMC-11140	Issue: When choosing "Export" from the Node Management menu while viewing a feature other than Node Management, the page may be remain blank or show a spinner indefinitely, although the export will succeed. Workaround: To avoid this, choose the "Node Management" menu option first, and after the page has loaded, choose "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.
ARCMC-7783	Issue: On the Monitoring page, the Connector Count can take a long time to update. Workaround: None.
ARCMC-6497	Issue: After adding a connector to a localhost container, listing all destinations from which to make a selection from may take some time. Workaround: None.

Issue	Description
ARCMC-4114	Issue: If the location of Logger nodes is updated, the new location will not be reflected in the path of the Logger initial configuration source nodes. Workaround: None.
ARCMC-2129	Issue: 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. Workaround: 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.
ARCMC-14311	Issue: When a new certificate is uploaded, the previously uploaded certificate is not deleted from the truststore. Workaround: Delete the previously added certificate from the truststore from command line and restart web.

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 2.81)

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 arc-doc@hpe.com.

We appreciate your feedback!