Micro Focus
ArcSight Management Center

Software Version: 2.91

Release Notes

Document Release Date: April, 2019
Software Release Date: April, 2019

Legal Notices

Copyright Notice

Trademark Notices

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:

- **Set Generator ID during Scan Host**

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

- "Fixed Issues" on page 10.
- "Open Issues" on page 11.
- "Security Fixes" on page 15.

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) 6.10, 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. For appliance upgrade: Red Hat Enterprise Linux 6.10, 7.6.
Client System	• Windows 7, 8, 10 • RHEL 6.9, 7.3, 7.4, 7.5.
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 6.10; all models C660x running RHEL 7.5.

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, v2.91
ArcMC	v2.2 or later.	v2.1 or later on models C650X and C660X.	v2.71, v2.91
Event Broker	v2.0 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 2.91 Software Depot at https://entitlement.mfgs.microfocus.com. The installer files for ArcSight Management Center 2.91 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.91.<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 v2.1 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-2.91.<build number>.0.bin`.

ArcMC Appliance OS Upgrade Files

The OS Upgrade files are available for download from the ArcMC 2.91 Software Depot at https://entitlement.mfgs.microfocus.com. The OS upgrade files for ArcSight Management Center 2.91 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 2.80 to software ArcSight Management Center 2.91. You should also upgrade any managed ArcMCs to version 2.91 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.91.

- **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 2.91:

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-2.91.<build number>.0.bin
   ```

```
./ArcSight-ArcMC-2.91.<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 SMPT 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-15271	Monitor and breach data purged in ArcMC 2.90 was failing. This is no longer happening.
ARCMC-15257	ArcMC 2.90 web UI was blank after upgrading ArcMC from 2.81. This was fixed in ArcMC 2.90 patch release.
ARCMC-15145	When a connector 7.11 was being added to ArcMC 2.9 with the Generator ID Management feature enabled, the ArcMC showed a message with 2 typos. This is no longer happening.
ARCMC-15137	After editing and trying to save a user group, an error window was displayed preventing the save process. This is no longer happening.
ARCMC-15091	The installation of the latest ArcMC build in a VM without the unzip and fontconfig commands was not working. This is no longer happening.
ARCMC-15049	When backup fails due to invalid directory path, no Audit log was generated. This is no longer happening.
ARCMC-14904	Installing a collector Syslog NG Daemon with TLS protocol was failing on the last step when doing it through 1-Click deployment. This is no longer happening.
ARCMC-14626	When arrows point to the topic boxes they pointed to the bottom of the box instead of the middle of it. This was fixed and now the arrows point to the middle of the box.
ARCMC-14348	ArcMC now supports the following connector property update on connector release >= 7.12 agent[*].enabled=false
ARCMC-14311	If the user uploaded an invalid certificate the service would continue working, now the SMTP service works only when a valid certificate is uploaded.
ARCMC-13869	UserMgmt Compliance report wasn't able to handle large size PDF files. This is no longer happening.
ARCMC-3822	Audit log now displays the actual user who performs FTP functions.

Open Issues

This release contains the following open issues.

Issue	Description
ARCMC-15266	Issue: When a rules file is imported into the system and it doesn't have all the required property fields for each rule, the system will throw a 500 error and the page will not be able to load the contents again until a new file is imported with all the necessary fields. Workaround: Re-upload a non corrupt file. Do not partially delete a rule from the exported breach rules file. The rules file to be uploaded should have all the properties for all the rules in the file. Before uploading a new breach rules file make a backup of the existing file.
ARCMC-15180	Issue: The monit log shows that APS and postgresql restart after stopped by `monit stop all.` Workaround: 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`.
ARCMC-14580	Issue: The Not operator cannot be used for creating rules from ArcMC to Event Broker. Workaround: None available at this time.
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-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.

Issue	Description
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.
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-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 available at this time.
ARCMC-12861	Issue: When Collector metrics are shown, the restart count is always 0. Workaround: None available at this time.

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. Workaround: 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.
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".

Issue	Description
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.
ARCMC-7783	Issue: On the Monitoring page, the Connector Count can take a long time to update. Workaround: None available at this time.
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 available at this time.
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 available at this time.
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.

Security Fixes

The following security fix was implemented in this release.

PSRT Case	Description	CVE
PSRT110647	Stored Cross-Site Scripting	CVE-2019-3486

Special thanks to ING Tech Poland 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 2.91)

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!