



**Hewlett Packard**  
Enterprise

# **HPE ArcSight ArcSight Management Center**

Software Version: 2.70

## Release Notes

October 19, 2017

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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 2017 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HPE ArcSight Technical Support Page: <a href="https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hpe.com">https://softwaresupport.hpe.com</a>
<b>Protect 724 Community</b>	<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>

# Contents

- About ArcSight Management Center ..... 4
- What's New in this Release ..... 5
- CEB and Collectors: For Testing and Evaluation Only ..... 6
- Technical Requirements ..... 7
  - For ArcSight Management Center ..... 7
  - For Managed ArcSight Products ..... 8
  - Installer Files ..... 8
  - ArcMC Appliance OS Upgrade Files ..... 9
  - Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x ..... 9
- Upgrading ArcMC .....10
  - Upgrade Prerequisites .....10
- Fixed Issues ..... 13
- Open Issues ..... 14
- Send Documentation Feedback ..... 17

# 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:

- **Instant Connector Deployment:** Deploy connectors and Collectors directly in the Deployment View where needed with just a few clicks, using the new Deployment Templates feature.
- **Deployment View:** The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations. Use the deployment view to model subsystems, and quickly trace issues and drill down on details.
- **Connectors in Event Broker (CEB):** ArcMC now includes the alpha Connectors in Event Broker (CEB) feature, **for non-production public alpha testing and evaluation**, which collects raw data through a source topic in Event Broker. Raw events are sent to this source topic from a Collector device. CEBs enable event normalization and processing to be moved directly to Event Broker. For restrictions on the alpha feature, see [About CEB](#) for more information.
- **ArcSight Secure Data Add-On Integration:** Deploy the ArcSight Secure Data Add-On encryption client to connectors and Collectors as part of Instant Connector Deployment. Events will be displayed in encrypted format in Logger and the ESM console.

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](#).

# CEB and Collectors: For Testing and Evaluation Only

Connectors in Event Broker (CEB) and all related functionality, including Collectors, are provided as **non-production public alpha features**. These features are provided for your testing and evaluation only and should not be considered fully functional, nor are they supported by HPE Support, nor are they guaranteed to be available in the product in the future.

Consult the ArcMC Admin Guide, and directions from the ArcMC product team, for best practices and guidance on how to use these features.

**CEB and Collectors must not in any circumstances be used in a production environment.**

We welcome questions, comments, and feedback on these features. Please direct any questions or comments to our ArcMC product team at [adp-ceb-alpha@hpe.com](mailto:adp-ceb-alpha@hpe.com).

# Technical Requirements

## For ArcSight Management Center

<b>Server</b>	<p>For software form factor:</p> <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux (RHEL) 6.9, or 7.3</li><li>• CentOS 6.9, or 7.3</li></ul> <p>For appliance upgrade: Red Hat Enterprise Linux 6.9 or 7.3*</p> <p>*Additionally, for RHEL7.x installation of software ArcMC: See <a href="#">"Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x" on page 9.</a></p>
<b>Client System</b>	<ul style="list-style-type: none"><li>• Windows 7, 8, 10</li><li>• MacOS 10.8 or later</li><li>• RHEL 6.9 or 7.3</li></ul>
<b>CPU</b>	1 or 2 Intel Xeon Quad Core (or equivalent)
<b>Memory</b>	<ul style="list-style-type: none"><li>• 16 GB RAM</li><li>• 80 GB Disk Space (for software form factor)</li></ul>
<b>Supported Client Browsers</b>	<ul style="list-style-type: none"><li>• Internet Explorer 11</li><li>• Microsoft Edge (version current as of release date) New features in this release are not supported on the Edge browser.</li><li>• Firefox ESR (version current as of release date)</li><li>• Google Chrome (version current as of release date)</li></ul>
<b>Screen Resolution</b>	Optimal screen resolution is 1920x1200
<b>Hardware Models</b>	For new and upgraded ArcMC appliance deployments, all models C650x running RHEL 6.9 and models C660x running RHEL 7.3

## For Managed ArcSight Products

Managed Product	Software Form Factor	Hardware (Appliance)	ArcMC Agent Version Required
<b>SmartConnector</b>	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.
<b>Logger</b>	v6.2, v6.2 P1, v6.3, v6.3.1, v6.4	v6.1, v6.1 P1, v6.2, v6.2 P1, v6.3, and v6.3.1 on models LX50X and LX60X	v2.70
<b>ArcMC</b>	v2.2, v2.2 P1, v2.5, v2.5.1, v2.6, v2.61 v2.70	v2.1, v2.2, v2.2 P1, v2.5, v2.5.1, v2.6, 2.61, v2.7.0 on models C650X and C660X.	v2.70
<b>Connector Appliance</b>	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX400 or CX500	v2.70
<b>Event Broker</b>	v2.0, v2.01, v 2.10	N/A	ArcMC Agent is not required
<b>Collector</b>	v7.7	N/A	ArcMC Agent is not required

## Installer Files

Available from the HPE download site, the installer files for ArcSight Management Center 2.70 are named as follows:

- **For Software ArcMC:** ArcSight-ArcMC-2.7.0.<build number>.0.bin
- **Software remote installer for use with the ArcMC Node Management:** 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-2.7.0.<build number>.0.bin`.

## ArcMC Appliance OS Upgrade Files

Available from the HPE download site, the OS upgrade files for ArcSight Management Center 2.7.0 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.9: (C650x appliances)** `osupgrade-arcmc-rhel69-<timestamp>.enc`
- **For Upgrade to RHEL 7.3: (C660x appliances)** `osupgrade-arcmc-rhel73-<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 2.60 or 2.61 to software ArcSight Management Center 2.70. You should also upgrade any managed ArcMCs to version 2.70 as well.

## Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.70.

- **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 filenames 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 7.3 for ArcMC 2.6.

For instructions on how to apply an appliance OS upgrade locally, see [Upgrading ArcMC](#).

**Note:** For OS upgrade files for a software ArcMC host, contact your host 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 2.70:

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-2.7.0.<build number>.0.bin  
./ArcSight-ArcMC-2.7.0.<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 Agentg. For instructions on upgrading the ArcMC Agent on managed nodes, see the ArcMC Administrator's Guide.

# Fixed Issues

This release of ArcMC includes the following fixed issues.

Key	Release Note Description
ARCMC-12827	Marketplace certificate domain name is changed to "marketplace.microfocus.com" in ArcMC 2.7
ARCMC-12496	Add the parameter below to logger.properties to support ArcMC backup file to the remote window system: enable.backup.checkDir=false.
ARCMC-12213	An issue has been fixed that was preventing ArcMC backup to some server types, such as Tectia.
ARCMC-11953	An issue has been resolved where adding Windows hosts from ArcMC UI resulted in the wincagent having a null value assigned to the new added Windows host entry on agent.properties.
ARCMC-10643	In some cases, an ArcMC hardware appliance was not able to manage another ArcMC hardware appliance running the same code version. This has been fixed.
ARCMC-10355	In some cases, when an ArcMC has been upgraded from a connector appliance, a limited selection of destination types was available. This has been resolved with connector 7.7.x.
ARCMC-10178	Several ArcMC processes could be left running after the ArcMC appliance is stopped using monit and needed to be killed manually. This will no longer occur.
ARCMC-9287	Although ArcMC can be used to change the username used to authenticate to a connector, avoid this procedure, as the new value is merely stored in ArcMC and not actually changed on the connector.
ARCMC-8944	When platform:230 and platform:201 events are forwarded from Logger to an ESM manager, the device host name and device address were converted to localhost and 127.0.0.1, respectively. This issue has been fixed.

# Open Issues

This release of ArcMC contains the following open issues.

Key	Description
ARCMC-13044	Backups of ArcMC configuration to a Windows machine will fail. Workaround: Add the parameter below to logger.properties to support ArcMC backup file to the remote window system: enable.backup.checkDir=false then restart web process
ARCMC-13036	Importing hosts will not function for collectors.
ARCMC-13037	For instant connector deployment, a connector name may not contain a forward slash character.
ARCMC-13020	When a connector VM's SSH key pair is changed, the instant deploy fails during the Preflight job.  Workaround: In the ArcMC's VM, go to the path: /home/<non root user>/.ssh.  Open the file "known_hosts"  Delete the line with the IP or host name of the Connector's VM
ARCMC-13024	In some circumstances, after successfully deploying a connector with the SecureData add-on, the connector will not be shown as a managed host in ArcMC.  Workaround: Try adding the connector as a managed node manually.
ARCMC-13019	In some cases, when deploying multiple connectors, and the job fails, all connectors should be marked as failed but only a few are so marked, and the job hangs.
ARCMC-13011	If user sees this error message, they should manually try to add that connector as a managed node to ArcMC.(It happens when the remote mgmt cert is not actually downloaded to the arcmc trust store, but still the method/API returns true for cert download; and then it tries to add it as managed node..)
ARCMC-12994	In some cases, when adding an additional, supplementary file to a repository for use in deployment templates, the file is not available to the user when editing the template or during the actual deployment.  Workaround: Create a new deployment template with the new repository file.
ARCMC-12968	When deployment fails with the memory issue 'OSError: [Errno 12] Cannot allocate memory' all the following deployment will fail with the same reason.So, the workaround is to kill the ansible process when the ansible does not exit properly.  Workaround:1) SSH to ArcMC system.2) Enter the command 'ps-ef   grep <job_name>'. Job_name is the name of the deployment job.3) Get the process ID of the Ansible job which you got.4) Kill that particular job Id using the command 'kill -9 PID'
ARCMC-12950	In some cases, CEBs will not be recognized as Connectors when creating monitoring rules.

Key	Description
ARCMC-12926	Remote Instant Connector/Collector Deployment from an ArcMC running RHEL/CentOS 6.9 to a remote Windows machine is not supported.
ARCMC-12876	The following graphs under the Monitoring Detail Summary view do not apply to CEBs: Queue Rate, Queue Drop Count, Command Responses Processed.
ARCMC-12861	When Collector metrics are shown, the restart count is always 0.
ARCMC-12834	Please use the name (hostname or IP), whatever is present in the remote host's CN, when deploying a connector or Collector. If it fails to add as a managed node, please try to add again manually with the correct host and port details.
ARCMC-12787	if a user is logged into the ArcSight Installer UI and another user deploys a CEB from ArcMC, the user logged into the ArcSight Installer UI will be logged off.  Workaround: User can just re-login to the Installer UI again.
ARCMC-12785	A CEB name with special characters will show as agent name on the Connectors tab. Avoid using special characters when naming CEBs.
ARCMC-12599	In Internet Explorer 11, the Add button for connectors and collectors is disabled.
ARCMC-12282	In Internet Explorer, the Topology drill down view can freeze the application.
ARCMC-11220	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 only access to System Admin page, restart the aps process on Process Status page. Once aps process restarts and is running, restart the web process. You should now have access to all menus.
ARCMC-11219	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-11212	When using local authentication to log in, and the user checks the Forgot Password checklist, the copyright statement is cut off. This issue only occurs in Chrome and Firefox.
ARCMC-11140	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. To avoid this, choose the "Node Management" menu option first, and after the page has loaded, choose "Export".
ARCMC-10828	On the Hosts tab, selecting multiple hosts to delete will fail and only delete the first one selected.

Key	Description
ARCMC-10478	<p>After a product type ages out, the product type is permanently removed from ArcMC. To bring back the device type, update the DB entry as follows.</p> <p>Updating the DB directly to the existing entry:</p> <p>Run the following:</p> <p>On a Software arcmc:</p> <pre>{install directory}/current/arcSight/bin/psql rwdb web</pre> <p>On an Appliance arcmc:{install directory}</p> <pre>/local/pgsql/bin/psql rwdb web</pre> <p>Then run the sql:</p> <pre>UPDATE arcmc_monitor_device_timeout SET device_timeout='20', device_tracking='t', device_ageout_days='13' WHERE device_product='&lt;device product&gt;';</pre> <p>Note: the device_timeout and device age_out parameters should be set to the desired values</p> <p>type \q to quit</p> <p>Restart the web service after update.</p>
ARCMC-9225	<p>Enabling the demo CA certificate fails when editing the destination from the Connector Summary ESM destination in Node Management. Workaround: Perform the demo CA enablement operation by using the Certificates button for selected connectors.</p>
ARCMC-7783	<p>On the Monitoring page, Connector Count can take a long time to update. Please be patient while the count is updated.</p>
ARCMC-6497	<p>After adding a connector to a localhost container, listing all destinations to select from may take some time. Please be patient while the list of destinations is built.</p>
ARCMC-4114	<p>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.</p>
ARCMC-2783	<p>Under Administration &gt; Network &gt; System DNS, the primary and secondary DNS should be set to 0.0.0.0 instead of letting them be empty fields. Setting the fields to an empty string causes issues with the DNS provider.</p>
ARCMC-2129	<p>In some circumstances, 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.</p>



# 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 system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Release Notes (ArcSight Management Center 2.70)**

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](mailto:arc-doc@hpe.com).

We appreciate your feedback!