



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight ArcSight Management Center**

Software Version: 2.61

Release Notes

July 12, 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
- Technical Requirements ..... 6
  - For ArcSight Management Center ..... 6
  - For Managed ArcSight Products ..... 7
  - Installer Files ..... 7
  - ArcMC Appliance OS Upgrade Files ..... 8
  - Prerequisite for ArcMC Installation or Upgrade for RHEL 7.x ..... 8
- Upgrading ArcMC ..... 9
  - Upgrade Prerequisites ..... 9
- Fixed Issues ..... 12
- Open Issues ..... 13
- 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 Event Broker, Loggers, Connectors, Connector Appliances, and other ArcMCs.
- **SmartConnector Hosting:** for the hardware appliance, as a platform to instantiate (host and execute) 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 resolves functionality and security issues present in ArcMC 2.6. For detailed information about ArcMC 2.6 features and functionality, refer to the ArcMC 2.6 Administrator's Guide, and other documentation, available from the [ArcSight Product Documentation Community](#).

# 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 6.8, 6.9, or 7.3</li><li>• CentOS 6.8, 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 8.</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)</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	v2.6.0
<b>ArcMC</b>	v2.2, v2.2 P1, v2.5, v2.5.1, v2.6	v2.1, v2.2, v2.2 P1, v2.5, v2.5.1, v2.6, v2.6.1 on models C650X and C660X.	v2.6.0
<b>Connector Appliance</b>	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX400 or CX500	v2.6.0
<b>Event Broker</b>	v2.0, v2.01, v 2.10	N/A	ArcMC Agent is not required

## Installer Files

Available from the HPE download site, the installer files for ArcSight Management Center 2.61 are named as follows:

- **For Software ArcMC:** ArcSight-ArcMC-2.6.1.<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-2.6.0.2005.0.bin`.

## ArcMC Appliance OS Upgrade Files

Available from the HPE download site, the OS upgrade files for ArcSight Management Center 2.61 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.9: (C650x appliances)** `osupgrade-arcmc-rhel168-  
<timestamp>.enc`
- **For Upgrade to RHEL 7.3: (C660x appliances)** `osupgrade-arcmc-rhel173-  
<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 2.6 to software ArcSight Management Center 2.61. You should also upgrade any managed ArcMCs to version 2.61 as well.

## Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.61.

- **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 2.61:

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-2.6.1.<build number>.0.bin
./ArcSight-ArcMC-2.6.1.<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

ArcSight Management Center 2.61 includes the same version of the ArcMC Agent as was included in ArcMC 2.6.0. Consequently, after upgrading to ArcSight Management Center 2.61, you will not need to upgrade the ArcSight Management Center Agent previously managed hosts in order to continue management.

# Fixed Issues

This release of ArcMC includes the following fixed issues.

Issue	Description
ARCMC-11642	In ArcMC 2.6, the built-in Marketplace certificate was only valid for 1 year and expired in June 2017, which caused an error of "Invalid Marketplace certificate not found" error displayed on the issue column of "Localhost". The issue is resolved.
ARCMC-11477	An issue has been resolved where an SNMP connector could fail to work with ArcMC 2.6.
ARCMC-11342	When adding a Logger to be managed by ArcMC, license tracking for the day the Logger is added will include all Logger ingestion since the last up time for the logger. This can appear as a big spike of data, but does not accurately reflect actual ADP managed data ingestion.
ARCMC-11224	The ArcMC Installer pre-flight check was not properly enforcing the upgrade path (ArcMC 2.5.1 to 2.6), and thus upgrade would fail on G8 appliances. This issue has been resolved and upgrade will no longer fail.
ARCMC-10736	In some cases, an error could occur on the Process Status page, showing incorrect uptime, under System Admin after upgrading the version of RHEL OS on an ArcMC appliance.
ARCMC-7898	The Apache process would fail to start if "Client Certificate" or "Client Certificate AND User Password" had been enabled before Trusted Certificates were uploaded.
ARCMC-10737	In some cases, an error message of "Sorry, there was an error" could occur on Connector Details page. This issue has been resolved.
ARCMC-11514	In some cases, when the number of device monitored by ArcMC was changes, the arcmc web service return an Out of Memory issue. The issue has been resolved.

# Open Issues

This release of ArcMC contains the following open issues.

Issue	Description
ARCMC-11219	<p>In some cases, a Kafka timeout causes an intermittent topic bootstrap failure. Because of this, Event Broker route creation in ArcMC may fail.</p> <p>Workaround: Restart webservices on the Event Broker master node.</p>
ARCMC-11212	<p>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.</p>
ARCMC-11174	<p>In some cases, adding a G8 Logger 6.31 to ArcMC as a managed host may return an Error 500 Internal Server Error.</p> <p>Workaround: Modify the iptables to reject instead of drop packets to unused ports as follows:</p> <ol style="list-style-type: none"><li>1. Ensure that ssh access is enabled in System Admin</li><li>2. On the logger appliance host, run the following commands at the command line: <code>iptables --append INPUT -j REJECT --reject-with icmp-port-unreachable</code></li></ol>
ARCMC-11140	<p>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".</p>
ARCMC-11133	<p>In the Topology View, the Event Broker destination for a managed Event Broker will appear to be unmanaged. To view the Event Broker metric details page, on the Dashboard, click the EB Nodes tile at the top of the page.</p>
ARCMC-11220	<p>On a freshly imaged ARI for ArcMC 2.6, when you restart the web process for the first time, you will have access to only System &amp; Admin page and no access to navigational menus.</p> <p>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.</p>

Issue	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:{install directory}/current/arcSight/bin/psql rwdb web</p> <p>On an Appliance arcmc:{install directory}/local/pgsql/bin/psql rwdb web</p> <p>Then run the sql:UPDATE arcmc_monitor_device_timeout SET device_timeout='20', device_tracking='t', device_ageout_days='13' WHERE device_product='&lt;device product&gt;;</p> <p>Note: the device_timeout and device_age_out parameters should be set to the desired value type \q to quite Restart the web service after update.</p>
ARCMC-10355	<p>In some cases, when an ArcMC has been upgraded from a connector appliance, only a limited selection of destination types (3) is available. Workaround: Edit “agent.properties” and append a new destination string (e.g: loggersecurepool, the string is dedicated for “logger secure pool” destination) to the end of the entry of “transport.types”, and then restart the container. Note that when modifying agent.properties to include the new destinations, those new destinations must be supported on the current container build.</p>
ARCMC-10256	<p>Only the 64-bit version of the Checkpoint OPSEC NG connector is supported on hardware series C6600.</p>
ARCMC-10178	<p>Several ArcMC processes may be left running after the ArcMC appliance is stopped using monit.</p>
ARCMC-9287	<p>ArcMC can be used to change the username used to authenticate to a connector. However, the new value is merely stored in ArcMC and not actually changed on the connector.</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-8944	<p>When platform:230 and platform:201 events are forwarded from Logger to an ESM manager, the device host name and device address are converted to localhost and 127.0.0.1, respectively.</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 2.61)**

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!