HPE ArcSight ArcSight Management Center

Software Version: 2.5.1

Release Notes

Novermber 29, 2016

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 2016 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

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

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 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

The ArcSight Management Center 2.5.1 release provides the same functionality as ArcSight Management Center 2.5, introduces fixes for a number of bugs, and includes the following important security updates.

- New RHEL 6.8 and 7.2 operating o ystem upgrades address the Linux kernel vulnerability, CVE-2016-5195: Kernel Local Privilege Escalation "Dirty COW". For details, see https://access.redhat.com/security/cve/cve-2016-6304.

- The version of OpenSSL has been upgraded to 1.0.2j to address multiple vulnerabilities including CVE-2016-6304. For details, see https://www.openssl.org/news/secadv/20160926.txt.

Resolved issues are described under "Fixed Issues" on page 14. For detailed information about ArcMC 2.5 features and functionality, refer to the ArcMC 2.5 Administrator's Guide, and other documentation, available from the ArcSight Product Documentation Community on Protect 724.

Additionally, a new bulk license installer tool is included with your download. Use this tool if you need to update or install more than one license at a time. The tool and a readme file that explains how to use it are included in the package `bulk-license-installer.zip`.

Technical Requirements

For ArcSight Management Center

Server	For software form factor:
	• Red Hat Enterprise Linux 6.8 or 7.2*
	• CentOS 6.8 or 7.2*
	For appliance upgrade: Red Hat Enterprise Linux 6.8 or 7.2*
	*Additionally, for RHEL7.x installation of software ArcMC: See *"Prerequisite to Installation for RHEL 7.x" on page 8*.
Client System	• Windows 7, 8, 10
	• MacOS 10.8 or later
	• RHEL 6.8 or 7.2
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 9/15/2016)
	• Firefox ESR (version current as of 9/15/2016)
	• Google Chrome (version current as of 9/15/2016)
Screen Resolution	Optimal screen resolution is 1920x1200
Hardware Models	For new and upgraded ArcMC appliance deployments, all models C650x running RHEL 6.8 and models C660x running RHEL 7.2

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 Connector Appliance, Logger (L3XXX), or separate server.	N/A	ArcMC Agent is not required.
Logger	v6.1, v6.1 P1, v6.2, v6.2 P1, v6.3, v6.3.1	v6.1, v6.1 P1, v6.2, v6.2 P1, v6.3, and v6.3.1 on models LX50X and LX60X	v2.5.1
ArcMC	v2.1, v2.2, v2.2 P1, v2.5, v2.5.1	v2.1, v2.2, v2.2 P1, v2.5, and v2.5.1 on models C650X and C660X.	v2.5.1
Connector Appliance	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX200, CX400, or CX500	v2.5.1

Installer Files

Available from the HPE download site, the installer files for ArcSight Management Center 2.5.1 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.5.1.1931.0.bin`
- **Software remote installer for use with the ArcMC Node Management:** `arcmc-sw-1931-remote.enc`
- **For ArcMC Appliance:** `arcmc-1931.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-2.5.1.1931.0.bin`.

ArcMC Appliance OS Upgrade Files

Available from the HPE download site, the OS upgrade files for ArcSight Management Center 2.5.1 Appliance (only) are named as follows:

- **For Upgrade to RHEL 6.8: (C650x appliances)** `osupgrade-arcmc-rhel68-20161108043353.enc`
- **For Upgrade to RHEL 7.2: (C660x appliances)** `osupgrade-arcmc-rhel72-20161108045103.enc`

> For OS upgrade files for a software ArcMC host, contact your host vendor.

Prerequisite to Installation 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 2.5 to software ArcSight Management Center 2.5.1. You should also upgrade any managed ArcMCs to version 2.5.1 as well.

Upgrade Prerequisites

Be sure that you meet these prerequisites before upgrading to ArcMC 2.5.1.

- **ArcMC Appliance OS Upgrade:** Upgrade the appliance OS to a supported OS version before upgrading the ArcMC version.

    Note: Be sure to apply the OS upgrade even if you already upgraded the OS to 6.8 or 7.2 for ArcMC 2.5, because the latest OS includes important security updates.

    OS support and required OS upgrade filenames are listed under Technical Requirements. For instructions on how to apply the appliance OS upgrade locally, see Uploading a License.

    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 2.5.1 using the install wizard:

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-2.5.1.1931.0.bin`

   `./ArcSight-ArcMC-2.5.1.1931.0.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**.

8. On ArcMC appliances, perform the following steps to configure the firewall:

   a. Log into the appliance as root.

   b. Run the following command:

      `[root@myserver ~]# /usr/sbin/arcfirewall --set`

      > **Note:** You must manually configure the firewall on software ArcMC.

Upgrading the ArcMC Agent

ArcSight Management Center 2.5.1 can only manage nodes that are running ArcSight Management Center Agent version 2.5.1. Consequently, after upgrading to ArcSight Management Center 2.5.1, you may also need to upgrade the ArcSight Management Center Agent on some or all previously managed hosts in order to continue management.

An Agent upgrade is required for any of the following host types running ArcSight Management Center Agent 2.0 or earlier that you wish to continue managing:

- **Hardware Appliances:** Hardware Connector Appliances, Logger Appliances, or ArcMC Appliances
- **Software Form Factors:** Software Connector Appliances, Software Loggers, or software ArcMCs

Agent Upgrade Procedure

ArcSight Management Center 2.5.1 can remotely upgrade the ArcMC Agent on any number of managed hosts. For ArcMC Agent upgrade instructions, see the ArcSight Management Center 2.5 Administrator's Guide.

Uploading a License

To upload your new license:

1. If you have not already done so, redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to ArcSight Management Center. For more information, refer to the software delivery confirmation email you received from HPE.

2. From the computer to which you downloaded the update file, log in to ArcSight Management Center using an account with administrator (upgrade) privileges.

3. Click **System Admin** from the top-level menu bar.

4. Click **License & Update** in the **System** section.

5. Browse to the license file you downloaded earlier, and click **Upload Update**. The Update in Progress page displays the update progress.

After you upload your license, reboot the ArcMC Appliance or restart software ArcMC. This restarts all processes with the new license settings.

Documentation Errata

The ArcMC 2.5 documentation contains the following errata.

- **Marketplace URL in Online Help:** In the online help, the link to the ArcSight Marketplace is incorrect. The correct Marketplace URL is https://marketplace.saas.hpe.com/arcsight.
- **Upgrading a Logger:** In the Upgrading a Logger section, in the table showing the upgrade files for each form factor, the entries in the column **Can Upgrade To Version...** should read "6.1 *or later*."
- **Installing Software Logger:** The Software Installation section of the ArcMC 2.5 Administrator's Guide gives incorrect syntax for setting limits in `/etc/security/limits.conf`.

  When creating or updating `limits.conf`, use the following lines instead of the text given in the Administrator's Guide.

```
* soft nofile 65536
* hard nofile 65536
```

> **Caution:** Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system run time errors.

Fixed Issues

The following issues are fixed in this release.

Issue	Description
ARCMC-9675	In some cases, on an ArcMC 2.5 enabled as ADP License Server, after installing a group of licenses, ArcMC System Admin would display the license status as invalid even though valid licenses exist on the server. Fix: On ArcMC 2.5.1 enabled as an ADP License Server, after installing a group of licenses, ArcMC System Admin will now correctly display the License Status as valid.
ARCMC-9674	On ArcMC 2.5, when there were more than 10 licenses installed, installing an Autopass license on the System Admin > License and Update page could take several minutes. Fix: Installing an Autopass license will now proceed quickly even if there are more than 10 licenses already installed. Additionally, for installing multiple Autopass licenses, a bulk license installer tool is provided, which can be run from the command line.
ARCMC-9532	ArcMC did not have the option to remain permanently on Daylight Savings Time (DST), which customers in Turkey now require. FIX: You now have the option to install an updated tzdata file during installation or upgrade, which resolves the issue. Users who do not need this fix can continue without the time zone upgrade.

Open Issues

This release contains the following open issues.

Issue	Description
ARCMC-9751	The Software Installation chapter of the 2.5 Administrator's Guide gives the incorrect syntax for setting limits in /etc/security/limits.conf. Workaround: When creating or updating the limits.conf, use the following lines instead of the text given in the Admin guide. * soft nofile 65536 * hard nofile 65536 Caution: Be sure to include the asterisk (*) in the new entries. It is important that you add all of the entries exactly as specified. Any omissions can cause system run time errors.
ARCMC-9741	On ArcMC 2.5 and 2.5.1, G8 appliances no longer respond to ICMP requests, such as ping requests. Workaround: This release includes an updated arcfirewall tool that you can use to resolve the issue. To enable the appliance to respond to ICMP requests, SSH as root to the appliance and run the command '/usr/sbin/arcfirewall --set'.
ARCMC-9695	When adding a connector to be managed by ArcMC 2.5, 2.5.1 license tracking for the day the connector is added will include all connector ingestion since the last Up time for the connector. This can appear as a big spike of data on the Monitoring page, but the spike does not accurately reflect actual ADP-managed data ingestion.
ARCMC-9287	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.
ARCMC-9235	In some cases, filters will not work correctly under the Property column on the Consumption Report.
ARCMC-9225	Enabling the demo CA cert 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.
ARCMC-9117	When ArcMC 2.5 enabled as ADP License Server is upgraded to ArcMC 2.5.1, the UI fails to display the accurate license limit GB/day on license usage graph on the Dashboard or on License information page under System Admin. It will display license limit as 0 GB in both places. Workaround: Once ArcMC 2.5 is upgraded to 2.5.1 and UI comes up, disable the ADP License Server check on Dashboard and enable the ADP License Server check again. After this step is completed, restart the aps process under Process Status under System Admin. Refresh the page, and you should be able to see the accurate license limit GB/day.

Issue	Description
ARCMC-9005	In the Topology view, if a connector has another connector as a destination, any devices sending events to the first connector will erroneously be shown as duplicate devices. The duplicates will be shown sending events to the destination connector.
ARCMC-8975	In some cases, when ArcMC 2.5 is freshly deployed on a Gen9 appliance, the user has only access to the System Admin Page. Workaround: Go to Process Status page and restart the aps process. Wait until aps process is up and running, and then restart the web process. After the web process is running, you should have access to all menus.
ARCMC-8944	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.
ARCMC-8781	In some cases, the topology view can be displayed twice. Workaround: If this occurs, click Refresh to show the correct view.
ARCMC-7898	The Apache process fails to start if "Client Certificate" or "Client Certificate AND User Password" has been enabled before Trusted Certificates are uploaded. Workaround: Apache will fail to start if the Trusted Certificates directory is empty. Upload Trusted Client certificates in the System Admin > Security > SSL Client Authentication > Trusted Certificates tab before enabling authentication methods from the System Admin > Users/Groups > Authentication > External Authentication tab.
ARCMC-7783	On the Monitoring page, Connector Count can take a long time to update. Please be patient while the count is updated.
ARCMC-6502	When Logger Event Archives have long names, the name may be displayed incorrectly. Workaround: To display the very long name of a Logger Event Archive, increase the width of the column.
ARCMC-6497	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.
ARCMC-6195	Using table filters on Monitoring > Summary and Monitoring > Product pages hides all data in the tables. Workaround: Refresh these pages to see the entire list of data in these tables.
ARCMC-4114	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. No workaround found.
ARCMC-4077	In Internet Explorer 11, when selecting multiple rows with the mouse, the text in the rows also is highlighted. This has no impact on the actual row selection other than to highlight the text. Workaround: Use SHIFT+arrow keys to select multiple rows.

Issue	Description
ARCMC-3977	Under Node Management, sorted lists do not save the user-preferred sort order.
ARCMC-2783	Under Administration > Network > 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.
ARCMC-2129	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.

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 2.5.1)

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!