Hewlett Packard
Enterprise

HPE Security ArcSight Management Center

Software Version: 2.2

Release Notes

March 21, 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 Security 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

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 Security ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

About ArcSight Management Center 2.2

ArcSight Management Center 2.2, one of the ArcSight Data Platform family of products, is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective manner.

ArcMC offers these key capabilities:

• **Management and Monitoring:** deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, 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

New Features and Enhancements

ArcSight Management Center 2.2 includes these new features and enhancements.

Logger Management

- **Logger Event Archive Management:** Remotely load, unload, and index Logger event archives.
- **Logger L3XXX Data Migration:** Support has been provided for data migration from Connector Appliance on L3XXX models to ArcSight Management Center. Instructions for this procedure are given in the Logger 6.2 Release Notes.

Monitoring

- **Pre-set Breach Rules:** ArcMC now ships with a variety of pre-set ("canned") breach rules, to cover a variety of performance metrics across managed devices.
- **Rules Enablement:** Existing rules can be enabled or disabled, as needed.

Configuration Management

- **FIPS Configuration:** New configuration types include FIPS configuration for managed nodes.

General

- **Localhost Remote Management:** The ArcMC localhost can now be added as a managed host and subscriber. The localhost can be managed through ArcMC and can be subscribed to configurations.
- **History Management:** Navigate more easily to previously-accessed pages by viewing previous pages in the node management tree or using the breadcrumb trail.
- **WINC Management:** Support has been added for WINC connector remote management and configuration.
- **Stats:** The new Stats menu shows Events Per Second In and Out for all managed connectors.
- **User Interface Improvements:** The UI has been improved and aligned with the modern, easy to use HP Enterprise look and feel.

Technical Requirements

For ArcSight Management Center:

These are the minimum system requirements for running ArcSight Management Center 2.2.

Server	For software form factor:

	• Red Hat Enterprise Linux 6.7 or 7.1 • CentOS 6.7 or 7.1 For fresh installation on appliance: Red Hat Enterprise Linux 7.1 For appliance upgrade: Red Hat Enterprise Linux 6.7
Client System	• Windows 7, 8, 10 • MacOS 10.8 • RHEL 6.4, 6.5, 6.6, 6.7
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 3/8/2016) • Firefox ESR (version current as of 3/8/2016) • Google Chrome (version current as of 3/8/2016) • Mac Safari 9
Screen Resolution	Optimal screen resolution for best view is 1920x1200
Hardware Models	• For new and upgraded ArcMC appliance deployments, all models 650x running RHEL 6.7

For Managed ArcSight Products

The supported version requirements for products managed by ArcSight Management Center are as follows:

Managed Product	Software Form Factor	Hardware (Appliance)	ArcMC Agent Version Required
Software Connector	v6.0.3 or later. Applies to software connectors running on Connector Appliance, Logger (L3XXX), or separate server.	N/A	None. ArcMC Agent is not required.
Logger	v6.0, v6.0P1, v6.0 P2, v6.1, v6.2	v5.5 P2, v6.0 + Bash vulnerability Hotfix+ Tzdata Hotfix, or v6.0 P1/6.0 P2, on models LX200, LX400, or LX500	v2.2
ArcMC	v2.0.x, v2.1, v2,2	v2.0.x,v2.1 or v2.2 on new model C6500, migrated model C6400.	v2.2
Connector	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX200, CX400, or	v2.2

Managed Product	Software Form Factor	Hardware (Appliance)	ArcMC Agent Version Required
Appliance		CX500	

Installer Files

Available from the HP download site, the installer files for ArcSight Management Center 2.2 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.2.0.<1646>.bin`
- **For ArcMC Appliance:** `arcmc-<1646>.enc`
- **ArcMC Agent Installer:** The ArcMC Agent installer for all appliance nodes, and for some types of software nodes, is bundled with the 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, a manual installer is required. The Agent installer file is required and named `ArcSight-ArcMCAgent-2.2.<1229>.bin.`

Upgrading ArcMC

Upgrade is supported from software ArcSight Management Center version 2.1 to software ArcSight Management Center2.2.

You should also upgrade any managed ArcSight Management Centers to version 2.2 as well.

Always perform any OS upgrade, if needed, to a supported OS version before upgrading the ArcMC version .

To upgrade to ArcSight Management Center 2.2:

1. Run these 2 commands from the directory where you copied the ArcSight Management Center software:

```
chmod +x ArcSight-ArcMC-2.2.0.<1646>.0.bin
./ArcSight-ArcMC-2.2.0.<1646>.0.bin
```

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

2. Follow the prompts to upgrade. For your installation directory, choose your original ArcSight Management Center installation directory.
3. If you run the ArcSight Management Center software installer as a non-root user:
   a. Specify an existing non-root user and to configure a port through which ArcSight Management Center users will connect through the UI. For example, you can enter 443, the standard HTTPS port, or any other that suits your needs. If any port other than 443 is specified, users will need to enter the port number in the URL they use to access the ArcSight Management Center UI.
   b. Enter the user name of the non-root user and the HTTPS port number, and then click Next. (These values may not be changed later in the process.)
4. Follow the prompts to complete product initialization.
5. If you run the installer as a root user, specify whether to run ArcSight Management Center as a system service or as a process.

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

Upgrading the ArcMC Agent

ArcSight Management Center 2.2 can only manage nodes that are running the ArcSight Management Center Agent version 2.2. Consequently, after upgrading to ArcSight Management Center 2.2, 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

Upgrade Procedure

ArcSight Management Center 2.2 can remotely upgrade the ArcMC Agent on one or multiple currently managed hosts, either software or appliance. For upgrade instructions, see the ArcSight Management Center 2.2 Administrator's Guide.

Fixed Issues

The following issues have been resolved in ArcSight Management Center 2.2.

Key	Release Note Description
ARCMC-5824	An issue has been fixed where ArcMC would not save ArcMC backup content option when the system was rebooted.
ARCMC-5624	The "Connector Detail" will now load and show the correct status of connectors more quickly.
ARCMC-5623	An issue has been resolved where the tooltip display would persist in the Node Management UI.
ARCMC-5264	Processing time on the Connector Detail page has been improved.
ARCMC-5121	On ArcMC G9 appliances, if FTP is enabled and successfully configured, the system admin UI no longer falsely reports that the FTP daemon is not running.
ARCMC-5067	If a container is backed up to a repository and then later restored into a repository, the container will no longer be listed twice.
ARCMC-4968	ArcMC will no longer return a compliance error if connector signature information is appended to the parser overwrite file.
ARCMC-4322	After a Logger Pool destination is added to a connector, when attempting to view the details on the connector detail page, an error message displayed.
ARCMC-4198	An issue has been resolved where an error (null) could occur if you upload a Connector AUP to a Connector Appliance 6.4 P3 which is later migrated to ArcMC 2.0 and then upgraded to ArcMC 2.1.
ARCMC-4154	During a push of a Logger initial configuration, the status icon would show In Progress. The correct status will now be shown.
ARCMC-4117	If a host certificate mismatch was reported, the dialog showing the mismatch would erroneously continue to display even if the issue is corrected. This issue has been fixed.
ARCMC-3934	An issue has been resolved where, during a backup/restore operation, ArcMC could become inaccessible and require a manual stop and start of ArcMC processes through SSH.
ARCMC-3900	If the connectors are processing heavy load of events, it is very likely that the connector upgrade will fail. So please stop the event flow on connectors before proceeding with connector upgrade.
ARCMC-	In some circumstances, after creating a search group on a Logger, importing it to a second Logger, and then

3862	pushing the group to a destination Logger, the search group would be incorrectly categorized as Shared on the destination Logger.
ARCMC-3732	On the node management tab, the title bar could be displayed incorrectly.
ARCMC-3146	You can now use the remote management Configuration Backup functionality to keep the backup content option as the original setting on a ConApp managed node when it is restarted.
ARCMC-3086	Immediately after installation, in some cases, the following message was displayed: "The requested URL's length exceeds the capacity limit for this server." This message is no longer displayed.
ARCMC-2855	The /etc/hosts file will now be restored from backup after a restore.
ARCMC-2838	In some cases, the Destinations button on the Connectors tab would not function when adding a destination.
ARCMC-2420	In some cases, while uploading an ENC file, although the upgrade completes, the upgrade status on the License and Upgrade page would still show as installing. This error has been corrected.
ARCMC-2010	The initial display of the Subscribers tab information for a selected Configuration on the Configuration Management page will now show the Subscribers list correctly.
ARCMC-1613	~~[CONAPP-4161]~~ Changes will now take effect if the year portion of the date is updated manually, using the ArcMC GUI.
ARCMC-1199	Previously, the scan host function would failed when the host had more than 21 containers. Such a scan will now be successful.
ARCMC-1055	~~[CONAPP-4577]~~ Connectors on local containers can now be restored after applying the backup.
ARCMC-812	A Syslog configuration can now be pushed to containers on the same host without causing a port conflict issue.

Open Issues

ArcSight Management Center 2.2 includes the following open issues. Use listed workarounds, where available.

Key	Release Note Description
ARCMC-6535	In some cases, when use ARCMC to push receivers to a target Logger, the receiver configuration files are generated but the pushed receivers are not populated on the target Logger UI. Workaround: Re-do the push of all missing receivers to the target logger.
ARCMC-6502	To display the very long name of a Logger Event Archive, please increase the width of the column.
ARCMC-6334	On the Event History page, when Cancel is clicked for Pending status, an incorrect job status is shown.
ARCMC-	When pushing an initial configuration containing SNMP destinations using ArcMC to Software Logger

6330	upgraded from 6.1 to 6.2, the Logger onboard connector process may fail to start after the push is completed and the Logger is rebooted. Workaround: Manually delete the pushed agent.properties (and the associated *.xml file, when there is SNMP destination in the pushed configurations) under <Logger install dir>/current/arcsight/connector/current/user/agent. After this, the OBC will auto-regenerate an initial agent.properties and user can manually add the SNMP destinations through the Logger UI.
ARCMC-6195	Using table filters on Monitoring > Summary and Monitoring > Product pages hides all data in the tables. The workaround is to refresh these pages to see the entire list of data in these tables.
ARCMC-6152	On some occasions, after navigating away from Node Management or completing an action like Add Host or Move on a node, a spurious error message is displayed which mentions parsing. The message can be ignored. Click "OK" to close the message and continue working.
ARCMC-6028	Deploying a FlexConnector and selecting Logger Poll as its destination will return an error.
ARCMC-6027	Using filters on the user list page works fine, but performing a delete operation on a filtered list displays an error. The workaround is to delete the users and user lists data without using filters on the user / user list table
ARCMC-5915	In Internet Explorer, on an upgraded ArcMC with many hosts, the exception error GetFrameFormName is sometimes displayed. To resolve this issue, clear the browser cache.
ARCMC-5913	In Configuration Management, when entering settings for a Logger Receiver configuration, a warning prompt is always displayed for the Logger Receiver name, even when the name is valid. Workaround: The configuration can still be saved even with the warning prompt displayed..
ARCMC-5625	In some cases, when there is complex data being loaded, the Node Management UI may take some time to display page data.
ARCMC-5299	When a role is created with a duplicate name of an existing role, the internal database error message, instead of a user-friendly error message, is displayed. Workaround: Do not use an existing role name when creating a role, or use Save As when creating a new role.
ARCMC-4275	After uninstallation of ArcMC, some files are not deleted. To delete the files, run these commands in the installation directory. chattr -ai current/local/monit/watchdog/apache.monitrc chattr -ai current/local/monit/watchdog/arcmc.monitrc chattr -ai current/local/monit/watchdog/monitrc_nonroot chattr -ai current/local/monit/watchdog/monitrc chattr -ai current/local/monit/watchdog/aps.monitrc chattr -ai current/local/monit/watchdog/postgresql.monitrc
ARCMC-4199	The container tooltip shows an erroneous FIPS status. Check the container properties to determine the correct FIPS status.
ARCMC-4196	After upgrading to ArcMC 2.1, CAC authentication no longer works. Workaround: Log in to the Logger UI as a user with administrator privileges, go to System Admin > SSL Client Authentication, delete and re-import all trusted certificates, and then restart apache.
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.

ARCMC-4087	In some cases, the repository files uploaded in Connector Appliance may not be correctly deleted and reuploaded. Workaround: 1. Delete the <versionInProblem> AUP from the Upgrade Files repository. 2. SSH to the box 3. Enter /opt/local/monit/bin/monit stop web 4. In the /opt/arcsight/userdata/arcmc/repository/upgrade/ folder, delete any leftover .tmp files 5. Mv all the *<versionInProblem>* connector files to another location 6. cd /opt/arcsight/userdata/arcmc/repository/upgrade/agents 7. mv all the *<versionInProblem>* connector files to another location 8. Make sure no files with <versionInProblem> in their name exist in the opt/arcsight/userdata/arcmc/repository/upgrade/ or in its subfolders 9. Enter /opt/local/monit/bin/monit start web 11. On the UI, re-upload the <versionInProblem> AUP again
ARCMC-4080	During a Logger Initial Configuration push, the /etc/hosts file of the destination loggers is replaced with the source logger's /etc/hosts file. So after the destination logger is configured using the Initial Configuration, login and manually edit the hosts file in the destination logger.
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.
ARCMC-3977	Under Node Management, sorted lists do not save the user-preferred sort order.
ARCMC-3719	In some cases, the following spurious error message may be displayed during installation: "SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder". SLF4J: Defaulting to no-operation (NOP) logger implementation SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details." This is a harmless error and can be ignored.
ARCMC-2969	Context sensitive help for the All Configurations and Repositories menu items will not show the correct help.
ARCMC-2783	Under Administration >Network >System DNS, both the primary and secondary DNS should be set to 0.0.0.0 instead of letting them be empty fields. Setting the fields to empty causes issues with DNS lookup.
ARCMC-2011	If creating a WUC external configuration with all the parameters given on ArcMC, please make sure all the parameters are also given on the connector side (while creating the connector). Otherwise the push or compliance check may fail.
ARCMC-1075	~~[CONAPP-4076]~~ In some cases, clicking the Previous button during the software upgrade may return this error message: "upgrade installation failed:Failure occurred at the following phase:init" Workaround: If this occurs, click Quit on the error dialog to cancel the installation. Then, restart the installation from the beginning.
ARCMC-1026	Turning interface homing on may result in a loss of connectivity to the appliance. If interface homing was already turned on and is known to be working, it can be left on. Workaround: If interface homing was turned on and connectivity was lost, it can be restored as follows: 1. In mouse/keyboard or iLO, log in to the console, and set the IP address of eth0 to its original address. This will cause the network service to be restarted and should restore network connectivity.

	2. Once network connectivity has been restored, point your browser to the appliance's web UI, log in, and go to Setup > System Admin > Network > NICs. Turn Interface homing off, and then restart the network service.
ARCMC-52	If pages are loaded in a small browser window, then maximizing the browser does not resize wizard pages correctly. Maximize the window and refresh the view to view a wizard page properly.

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 2.2)

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!