Release Notes

ArcSight Management Center 2.0 Patch 2

February 13, 2015

ArcSight
An HP Company

HP ArcSight Management Center 2.0 Patch 2 Release Notes

Revision History

Date	Product Version	Description
2/13/15	2.0 Patch 2	Revised and clarified upgrade instructions for software/hardware form factors.
12/8/14	2.0 Patch 2	Document release.
7/22/14	2.0	Revised release notes.
5/19/14	2.0	Initial document release.
9/30/13	1.0	Initial document release.

HP ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

HP ArcSight Management Center 2.0 Patch 2 Release Notes

These release notes provide current information about HP ArcSight Management Center 2.0 Patch 2. The following topics are discussed here:

About HP ArcSight Management Center 2.0 Patch 2

HP ArcSight Management Center 2.0 Patch 2 (2.0 P2) is a maintenance release that resolves all issues listed under "Fixed Issues" on page 13. In addition, it includes the most recent hotfixes released by HP ArcSight, as well as support for management of Logger 6.0 and 6.0 P1.

Patch 1: ArcSight Management Center 2.0 Patch 1 (2.0 P1) was a limited release that enhanced the ArcMC Agent to support management of Logger 6.0. These ArcMC Agent enhancements are included in ArcSight Management Center 2.0 Patch 2. Customers who applied ArcMC 2.0 Patch 1 with guidance from HP Support can freely upgrade to ArcMC 2.0 Patch 2.

Upgrade is supported for software ArcSight Management Center, as well as ArcSight Management Center Appliance.

Included Hotfixes

Hotfixes addressing the following issues are included in this patch:

- **Bash Code Injection Vulnerability:** This hotfix resolves the Bourne-Again Shell (Bash) Code Injection via Specially Crafted Environment Variables vulnerability on HP ArcSight Management Center model C6500 series appliances. This includes any appliance that was originally a Connector Appliance but was later migrated to ArcSight Management Center.

- **POODLE:** This hotfix resolves the POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability on HP ArcSight Management Center.
- **TZDATA:** This hotfix brings HP ArcSight Management Center into compliance with changes to time zones in the Russian Federation, which were scheduled to go into effect on October 26, 2014.

Customers who have previously applied any of these hotfixes may also freely apply this patch.

Support for Logger 6.0 and 6.0 P1

ArcMC Agent support has been added for remote management of Logger 6.0 and 6.0 P1. ArcMC Agent version 2.0 P2 must be running on the remotely managed Logger host in order to enable management.

Technical Requirements

For ArcSight Management Center

These are the minimum system requirements for running ArcSight Management Center 2.0 Patch 2.

Server	• Certified: Red Hat Enterprise Linux (RHEL) 6.4, 6.5 (64-bit) • Supported: CentOS 6.4,6.5
Client System	• Windows 7,8 • Mac OS 10.8 • RHEL 6.4, 6.5
CPU	1 or 2 Intel Xeon Quad (or equivalent)
Memory	• 8 GB RAM • 20 GB disk space (for software form factor)
Supported Client Browsers	• Internet Explorer 9, 10 • Mozilla Firefox ESR 31.2 • Chrome version 38 (version as of 11/20/2014)
Hardware Models	• For new deployments, model C6500 • For migrated deployments, model C6400

For Managed ArcSight Products

The supported version requirements for ArcSight 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.
Connector Appliance	v6.4 P3 or v6.4 P3 (6885) Hotfix	v6.4 P3, on models CX200, CX400, or CX500	2.0 P2
Logger	v5.5P2, v6.0 or v6.0 P1	5.5 P2, v6.0 + Bash vulnerability Hotfix+ Tzdata Hotfix, or v6.0 P1, on models LX200, LX400, or LX500	2.0 P2
ArcMC	v2.0.x	v2.0.x on new model C6500, migrated model C6400.	2.0 P2

Installers

Available from the HP download site, the installer files for ArcSight Management Center 2.0 Patch 2 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.0.0.1397.2.bin`
- **For ArcMC Appliance:** `arcmc-1398.enc`
- **ArcMC Agent Installer:** `ArcSight-ArcMCAgent-2.0.0.1189.2.bin`

Upgrade Instructions

Upgrade is supported from Software ArcSight Management Center 2.0 (or 2.0 P1) to ArcSight Management Center 2.0 Patch 2.

In order to upgrade from ArcMC 1.0 to 2.0 P2, first upgrade to ArcMC 2.0, and then perform the upgrade described below to ArcMC 2.0 P2.

Upgrading from version 1.0 to version 2.0 is described in the ArcSight Management Center Release Notes, available from the HP ArcSight community, Protect724.

The upgrade procedure and required installer file depends on the form factor (software or hardware) of the ArcMC being upgraded. In addition, the ArcMC Agent may need to be upgraded on HP ArcSight products currently managed by ArcSight Management Center.

- For software ArcSight Management Center instructions, see “Upgrading Software ArcSight Management Center” on page 8.

- For ArcSight Management Center Appliance upgrade instructions, see "Upgrading an ArcSight Management Center Appliance" on page 11.
- For instructions on upgrading the ArcMC Agent on managed products, see "Upgrading the ArcMC Agent on Managed Products" on page 11.

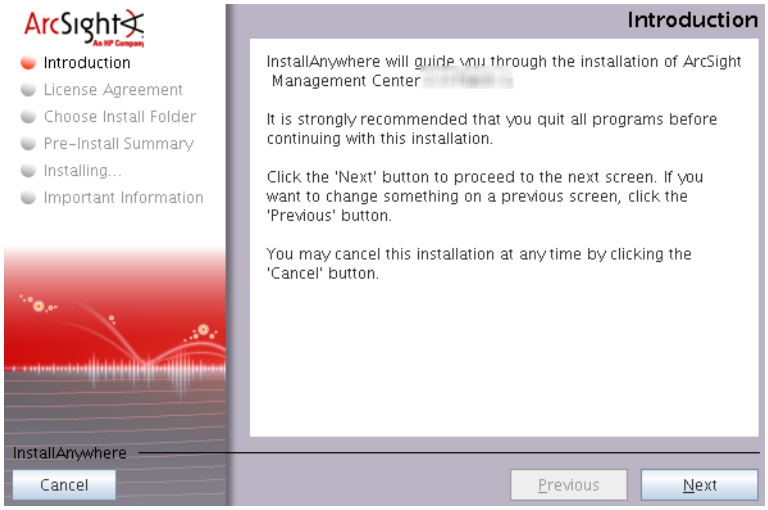
Upgrading Software ArcSight Management Center

To upgrade Software ArcSight Management Center 2.0 (or 2.0 P1) to 2.0 Patch 2:

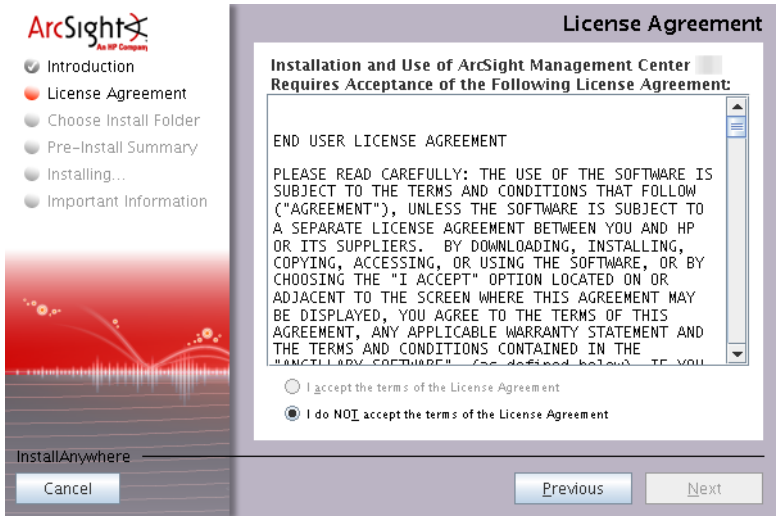
1. Run these 2 commands from the directory where you copied the Software ArcMC installer (named `ArcSight-ArcMC-2.0.0.1397.2.bin`):

   - `chmod +x ArcSight-ArcMC-2.0.0.1397.2.bin`
   - `./ArcSight-ArcMC-2.0.0.1397.2.bin`

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

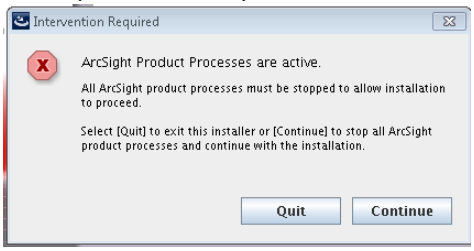


2. Review the License Agreement details, and then scroll down to the end of the License Agreement details. Select **I accept the terms of the License Agreement**. Then, click **Next.**

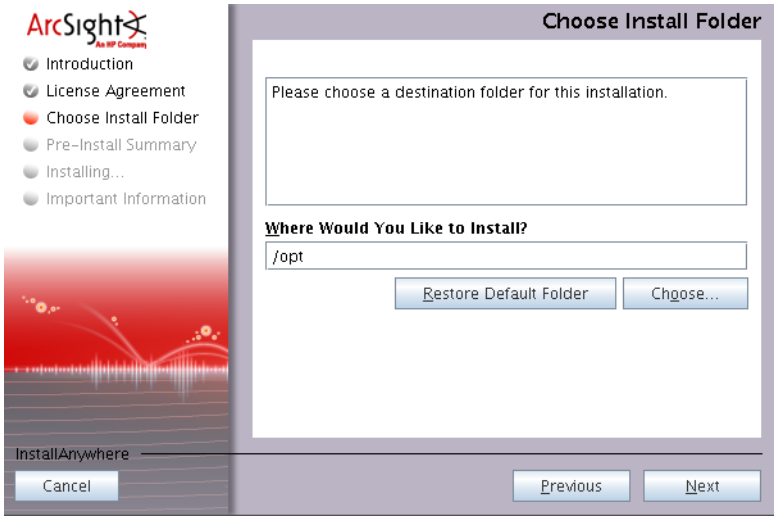


[

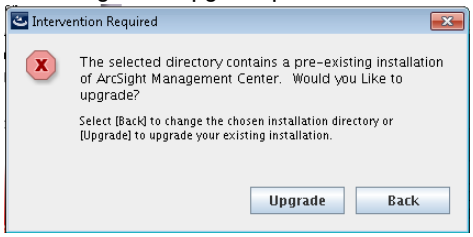
3 The installer will report that some processes are still active. Click **Continue**.



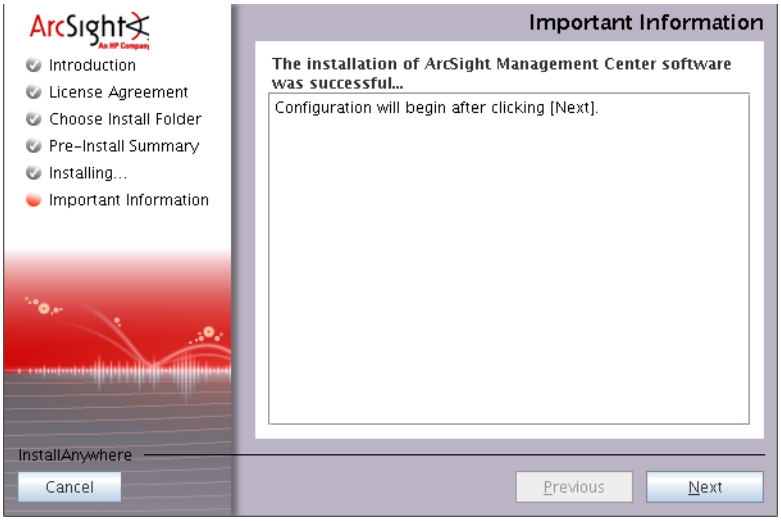
4 For your installation directory, choose your original ArcSight Management Center installation directory.



5 Click **Upgrade** to begin the upgrade process.



6 When the process is complete, click **Next** to begin the configuration wizard.



7 If you run the ArcSight Management Center software installer as a root user, the next dialog enables you to 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.

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.)

8 After the software is installed, click **Next** to begin ArcSight Management Center initialization.

9 After initialization is complete, click **Done** to launch the ArcSight Management Center Configuration wizard.

Note

The Configuration wizard should launch automatically. If it does not, use this command to launch the wizard:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup
```

10 If you have run the ArcSight Management Center software installer as a root user, the next dialog enables you to configure ArcSight Management Center to run as a system service or as a process.

When you configure ArcSight Management Center as a system service, a service called `arcsight_arcmc` will be configured and enabled at runlevels 3 and 5.

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`.

11 You have upgraded ArcSight Management Center. Click **Start** ArcSight Management Center **Now**, or click **Start** ArcSight Management Center **later,** and then click **Finish**.

12 If you selected **Start** ArcSight Management Center **Now**, click **Finish** to exit the wizard. Alternatively, wait for the next dialog which provides the URL to access the ArcSight Management Center interface.

ArcSight Management Center continues to start services and processes in the background.

Upgrading an ArcSight Management Center Appliance

To upgrade ArcSight Management Center Appliance 2.0 (or 2.0 P1) to 2.0 Patch 2:

1. Download the installer file (named `arcmc-1398.enc`) to a computer from which you can connect to the ArcMC appliance.
2. From the computer to which you downloaded the installer file, log in to the ArcMC appliance using an account with administrator (upgrade) privileges.
3. Click **System Admin** from the top-level menu bar.
4. Click **License & Update** from the **System** section.
5. Browse to and select the file you downloaded earlier, and click **Upload Update.**

   An **Update In Progress** page displays the update progress. Once the update has completed, the **Update Results** page displays the update results.

Upgrading the ArcMC Agent on Managed Products

ArcSight Management Center 2.0 P2 can only manage appliance or software nodes running ArcSight Management Center Agent 2.0 P2.

Consequently, after upgrading to ArcSight Management Center 2.0 Patch 2, any previously managed hosts running an earlier version of the ArcMC Agent may require an Agent upgrade to bring the version number to 2.0 P2.

Managed Hardware Appliances

ArcSight Management Center 2.0 P2 can remotely upgrade the ArcMC Agent running on any currently managed ArcMC, Connector Appliance, or Logger Appliance. For instructions, see the ArcSight Management Center 2.0 Administrator's Guide.

If the appliance was *not* previously managed by the upgraded ArcSight Management Center, and is still running ArcMC Agent 1.0, you can neither add the host directly to ArcSight Management Center 2.0 P2, nor upgrade the Agent. Instead, do the following:

1. Stop the ArcMC Agent process on the appliance (**System Admin > Process Status > Stop ArcMC Agent**).
2. Add the appliance host to your newly upgraded ArcSight Management Center. (See the Administrator's Guide for instructions on adding a host.) ArcSight Management Center will automatically install ArcMC Agent 2.0 P2 and will then manage the appliance.

Managed Software Form Factors

To upgrade the ArcMC Agent on a software form factor host (Software ArcMC, Software Connector Appliance, or Software Logger), do the following:

1. Uninstall the previous version of the ArcMC Agent.
2. Manually install the ArcMC Agent 2.0 P2.

For instructions on each of these procedures, see the ArcSight Management Center 2.0 Administrator's Guide.

Fresh Install of ArcSight Management Center 2.0 Patch 2

ArcSight Management Center 2.0 Patch 2 may be freshly installed on a host. To install ArcSight Management Center 2.0 Patch 2 as a fresh install, follow the instructions given in the “Software Installation” chapter of the ArcSight Management Center 2.0 Administrator’s Guide.

Available Documentation

In addition to these release notes, ArcSight Management Center documentation comprises the following, available from the HP ArcSight community, Protect724.

- The ArcSight Management Center 2.0 Administrator’s Guide, explaining features and functionality for ArcMC 2.0 P2.
- The ArcSight Management Center 2.0 Migration Guide, explaining procedures for migrating Connector Appliance 6.4P3 to ArcSight Management Center 2.0.
- Getting Started with ArcSight Management Center, explaining basic configuration steps for ArcMC appliances.

In addition, ArcSight Management Center includes Online Help, integrated into the product and available from the Help link in the upper-right of the browser window.

Documentation Errata

The documentation includes the following errata:

Issue	Description
ARCMC-2131	In the online help file, the breach rules file to be edited is incorrectly specified as exportrules.csv, instead of the correct name, monitor_breach_rules.properties. The file name is correctly noted in the Administrator’s Guide.
ARCMC-2132	In the online help file, under Monitoring, in the table for Breach Rules Parameters, supported severity levels should read WARNING, CRITICAL, and FATAL.
ARCMC-2353	If ArcSight Management Center is installed as a non-root user, and the host is rebooted, ArcMC services will fail to start automatically. Start them manually with this command: `<install dir>/current/arcsight/arcmc/bin/arcmcd start`
ARCMC-2472	Under Installation Prerequisites, under File Descriptors, change the word ‘nolimit’ to ‘nofile.’

Known Limitations

ArcSight Management 2.0 P2 includes the following limitations:

- To successfully upgrade a Logger Appliance to version 6.0 or later, make sure the ArcMC Agent running on the Logger Appliance is version 2.0 P2 or later.
- While upgrading ArcSight Management Center from 2.0 to 2.0 P2, Internet Explorer may hang and display a status of *In Progress.* If the condition persists for longer than 30 minutes, and there are no network issues, refresh Internet Explorer to display the correct status of the update.
- The System Admin UI will not be correctly displayed in Google Chrome version 39.

Fixed Issues

The following issues have been resolved in this release.

Issue	Description
ARCMC-2413	Whenever the ArcMC Agent is restarted, the status will correctly show as Running.
ARCMC-2313	After the migration of Connector Appliance to ArcMC 2.0 and subsequent upgrade to 2.0 P2, an admin user will have any missing rights restored. The rights of all other users will be unaffected.
ARCMC-2290	The Bourne-Again Shell (Bash) Code Injection Vulnerability via Specially Crafted Environment Variables on HP ArcSight Management Center model C6500 series appliances is resolved. This includes the following CVEs: • CVE-2014-6271 • CVE-2014-7169 • CVE-2014-6277 • CVE-2014-6278 • CVE-2014-7186 • CVE-2014-7187
ARCMC-2261	HP ArcSight Management Center is now compliant with changes to time zones in the Russian Federation, which were scheduled to go into effect on October 26, 2014.
ARCMC-2233	The POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability (CVE-2014-3566) is resolved.
ARCMC-2218	The ArcMCAgent can now be upgraded on all ArcMC Appliances.
ARCMC-2130	When a host is relocated from the default location, after rebooting, the host's model and version would previously be reported as Unknown.
ARCMC-2121	If a location was renamed, then after a reboot, the location would revert to its old name. This issue has been resolved. However, customers with ArcMC 2.0 will still see this issue. To avoid this issue, before renaming, upgrade to ArcMC 2.0 P1, and then perform the rename.
ARCMC-2082	Prompted pushes will now succeed if a subscriber is added to an updated configuration.
ARCMC-2052	On the Monitoring page, a warning will now be shown if the user attempts to upload an invalid file type. (Only CSV files with the extension `.properties` are valid.)
ARCMC-2050	An issue has been resolved when Setting a Configuration on a managed Logger, and invalid data was entered into a field. The Logger will no longer be shown in ArcMC with a incorrect status of Down.
ARCMC-1667	The Issue column on the host page will now correctly show a message when authentication fails.
ARCMC-1426	Previously an upgrade to a container in FIPS mode would fail. The upgrade will now succeed.
ARCMC-1367	Upon first installing a Syslog connector on ArcSight Management Center running on CentOS 6.5, a popup message would claim that CentOS is not supported. In fact, CentOS 6.5 is supported by ArcSight Management Center. This message was incorrect and will no longer be shown.

Issue	Description
ARCMC-1220	In some cases, during the import hosts process, the last host in the uploaded CSV file was not imported. The last host will now be imported correctly.
ARCMC-1108	In some cases, the Destinations button on the Connectors tab would not function when adding a destination.
ARCMC-346	When adding a host with multiple containers, only a single set of credentials (such as myusername/mypassword) may be passed to each container. As a result, the credentials of all containers on the host must all be identical, or the add host operation will fail. If they are not identical already, then change all container credentials to match one another.

Open Issues

This release contains the following open issues. Use the workarounds, where available.

Issue	Description
ARCMC-2490	In some cases, after deleting and then re-adding a host, a spurious error message will be displayed upon re-adding: "Failed to add host." This error message can be ignored.
ARCMC-2400	When the user changes the ArcMC service from " Don't start as a service " to "Start as a Service" (or the reverse) and then reboots the system, ArcMC processes will not automatically restart. Manually restart the services using the command: <install dir>current/arcsight/arcmc/bin/arcmcd start all.
ARCMC-2273	If the configuration on the managing ArcMC and subscriber configuration have same property sets, then the 'Check compliance' status is returned as 'Yes'; that is, compliant, irrespective of the order of property sets.
ARCMC-2051	Under Node Management > Edit/Update Configuration: if the user selects the storage group configuration type to be updated, the Add Row link is visible. This should not be the case. The link is to add new entries to storage groups, which is not supported in ArcSight Management Center. If the user proceeds with the operation, it will fail and no storage group configuration push will occur.
ARCMC-2039	Any change to a DNS entry requires a restart of the web process for all features and functions to work as expected.
ARCMC-2033	In some cases, when adding an FTP subdirectory with a special character (such as: ~ ! @ # $ % ^ & *) , an error message is returned that says "null." Workaround: Do not use special characters in an FTP subdirectory name.
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-1979	If a node is being restarted after having it added onto ArcMC, the status that will be displayed is "initialized" even though the node has not come up yet.

Issue	Description
ARCMC-1894	In the System Admin UI License & update page, if an error occurs when uploading a new license or update, the UI will report that an error occurred but it may not always display the actual error message. Workaround: Refresh the browser, go back to the License & Update page and click on the "Last Update Status" link.
ARCMC-1613	[CONAPP-4161] Changes will not take effect if the year portion of the date is updated manually, using the ArcMC GUI. Instead, change the entire date, and not just the year.
ARCMC-1373	In some cases, on a migrated ArcMC, when setting a value for a Network Configuration, ArcMC will report success when in actuality the value does not change.
ARCMC-1284	If an attempt is made to add a "CEF encrypted syslog" destination using the "choose from existing destination" option, then there is no way to enter the shared key value. Because of this, the destination is not registered correctly, resulting in caching of the events. Workaround: To add a "CEF encrypted syslog" destination, then use only the "create a new destination" option.
ARCMC-1057	[CONAPP-4573] An upgrade may fail if issued from the ArcMC GUI to a connector processing a heavy load of events. Workaround: If the upgrade fails from the ArcMC GUI by timing out, do one of the following: -Stop the event feed to the connector and let it process all the cached events. Then perform an upgrade from the Connector Appliance GUI, OR, -Back up the container, perform an emergency restore on it to the required build, and then restore the backed up files to the same container.
ARCMC-1055	[CONAPP-4577] Connectors on local containers may not be restored after applying the backup. Workaround: To restore a connector from the backup configuration, restart it. To restart a connector: 1. Click Setup > System Admin > Process Status. 2. From the list of connectors, select the connector to restart and then click the Restart button.

Issue	Description
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-653	It is a common practice to use an internal certificate authority to sign all certificates used within an organization. However, ArcSight Management Center does not currently support importing the internal certificate authority's root certificate into its trust store. Therefore, certificates signed by internal certificate authorities will be treated as untrusted. Workaround: Import each individual host certificate when prompted during the 'Add host' workflow.
ARCMC-652	A software connector added as a managed node will be displayed on the Hosts tab as "Software" instead of "Software Connector".
ARCMC-552	The Filter button does not operate in Internet Explorer 8. To use the Filter button, press F12, and then change the document mode to Internet Explorer 8.
ARCMC-304	In some circumstances, the navigation tree on the left is replaced with the content of the management panel on the right. The workaround is to log out and then log back in.
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.