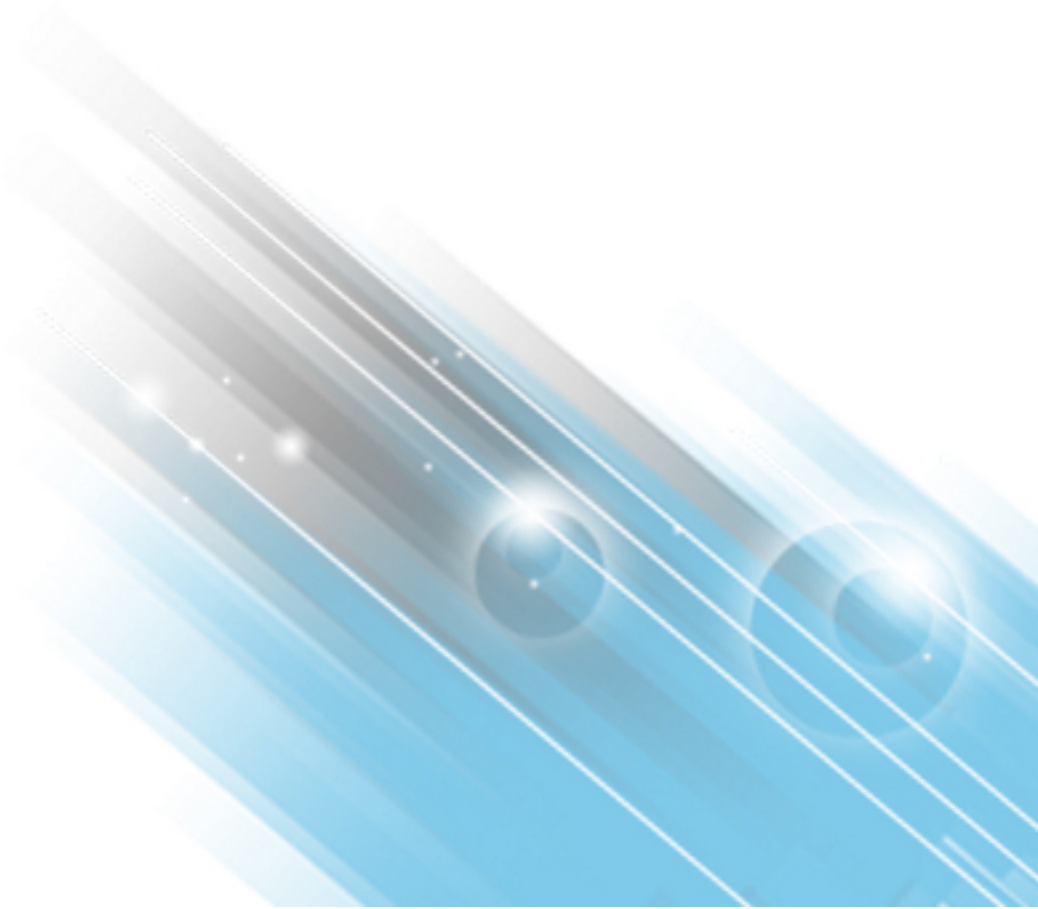
HP ArcSight Management Center

Software Version: 2.1

Release Notes



September 2, 2015

Legal Notices

Warranty

The only warranties for HP 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. HP 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.

HP 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 HP 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:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

Phone	A list of phone numbers is available on the HP 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://protect724.hp.com

Contents

About ArcSight Management Center 2.1

ArcSight Management Center 2.1 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 2.1 includes these new features and enhancements.

User Management

- **User Management**: Role-based access control (RBAC) user management enables you to manage user access with custom roles across specified nodes.

Logger Management

Logger management enhancements include:

- **Logger Initial Configurations:** An initial configuration is intended for the rapid, uniform setup of multiple HP ArcSight Loggers of the same model number and software version. Use an initial configuration to expedite the initial deployment of Loggers to a production environment. Initial configuration management is supported on Logger version 6.1 or later.
- **Logger Peer Management:** Logger peer management is supported. Peer Logger management in ArcMC is only supported for Loggers of version 6.1 or later. However, Logger peers may be of versions earlier than 6.1.
- **New Logger Configurations:** New Logger configurations include Logger Connector Forwarder, Logger ESM Forwarder, Logger TCP Forwarder, and Logger UDP Forwarder.
- **Bulk Logger Upgrade:** Upgrade multiple Loggers in bulk, from version 6.0 to 6.1.
- **Logger License Entitlement Report:** The new License Entitlement Report enables easy monitoring of licensed settings and your usage against your entitlements by managed Loggers.

Connector Management

Connector management enhancements include:

- **Destination Configurations**: The new destination configuration type enables you to set values for destination settings on connectors.
- **Network Model Support:** The new Networks and Zones configuration defines values and behavior for networks and zones, and can be pushed to connectors.

- **Enhanced Upgrade Status:** The details regarding connector status after an upgrade has been improved.
- **ArcSight Logger SmartMessage Pool (Encrypted) Destination:** ArcSight Logger SmartMessage Pool (Encrypted) is now supported as a connector destination type.

Configuration Management

New configurations are available for managed nodes.

- **Configuration Comparison:** Compare two configurations of the same type quickly, with a field by field breakdown of each setting, its value, and any differences. You can compare the values of a configuration on a subscriber node to the values of the baseline or reference configuration on an ArcMC which manages it. You can also compare two configurations of the same type on a single ArcMC.
- **New System Admin Configurations:** New system admin configurations include improved SNMP Trap Configuration, and the new SNMP Poll Configuration, both with SNMP version 3 support .

Monitoring

Monitoring now includes these features:

- **Rules Editor:** A new rules editor makes creation of new monitoring rules quick and easy. In addition, monitoring rules can now include notification by email, by SNMP, or through logs and audit forwarding.
- **Storage Group Capacity Monitoring:** Monitor the storage group capacity of managed Loggers.
- **Logger Forwarder Graph:** A new graph displays Logger forwarding activity graphically.

Node Management

Node management includes these enhancements:

- **Software Host Upgrade:** Software ArcMC and software Logger can now be upgraded remotely.
- **Automatic Installation of Agent on Software Hosts:** The Agent on software Logger 6.0 and later and software ArcMC and later can now be installed automatically upon adding the hosts for management.
- **Update Credentials:** Host authentication credentials can now be updated without having to re-add a host for which the credentials have changed.

Additional Enhancements

In addition, this version of ArcMC includes these enhancements:

- **Improved UI:** The user interface, navigation, and accessibility have been improved and streamlined.
- **Site Map:** A navigational site map improves accessibility to ArcMC functions.

Technical Requirements

For ArcSight Management Center:

These are the minimum system requirements for running ArcSight Management Center 2.1.

Server	For software form factor: • Red Hat Enterprise Linux 6.6 or 7.1 • CentOS 6.6 or 7.1 For appliance: • Red Hat Enterprise Linux 6.6
Client System	• Windows 7 or 8 • MacOS 10.8 • RHEL 6.4, 6.5, 6.6
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 10 or 11 • Firefox ESR 38 • Google Chrome (version current as of September 1, 2015) • Mac Safari 8
Hardware Models	For new and upgraded ArcMC appliance deployments, all models 650x running RHEL 6.6

For Managed ArcSight Products

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

Managed Product	Software Form Factor	Hardware (Appliance)	ArcMC Agent Version Required
Logger	v6.0, v6.0P1, v6.0 P2, v6.1	5.5 P2, v6.0 + Bash vulnerability Hotfix+ Tzdata Hotfix, or v6.0 P1/6.0 P2, on models LX200, LX400, or LX500	2.1
ArcMC	v2.0.x, v2.1	v2.0.x or 2.1 on new model C6500, migrated model C6400.	2.1
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	2.1

Installer Files

Available from the HP download site, the installer files for ArcSight Management Center 2.1 are named as follows:

- **For Software ArcMC:** `ArcSight-ArcMC-2.1.0.1497.bin`
- **For ArcMC Appliance:** `arcmc-1497.enc`
- **ArcMC Agent Installer:** `ArcSight-ArcMCAgent-2.1.1213.bin`

Upgrading ArcMC

Upgrade is supported from software ArcSight Management Center 2.0 or 2.0 P2 to software ArcSight Management Center2.1.

Note ArcSight Management Center 2.1 is supported on RHEL 6.6. If your ArcSight Management Center is running an earlier version of RHEL, you will need to upgrade the operating system to 6.6 **before** upgrading ArcSight Management Center.

- **For theArcSight Management Center** Appliance, you can download the OS upgrade file from the same location you downloaded the ArcSight Management Center software. The filename format for the OS upgrade file is `osupgrade-arcmc-rhel66-<build number>.enc`.
- **For software ArcSight Management Center***,* contact your OS vendor for the correct OS upgrade file.

To upgrade from ArcMCArcSight Management Center 1.0, first upgrade to version 2.0, then upgrade to 2.1.

To upgrade ArcSight Management Center 2.0 to 2.1:

1. Verify your system meets the operating system and other requirements for the new version, as shown under "Technical Requirements" on page 8. If necessary, upgrade your OS to a supported version.
2. Copy the ArcSight Management Center software to a secure network location.
3. Run these 2 commands from the directory where you copied the ArcSight Management Centersoftware:

```
chmod +x ArcSight-ArcMC-2.1.0.1497.0.bin
```

```
./ArcSight-ArcMC-2.1.0.1497.0.bin
```

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

4. Follow the prompts to upgrade. For your installation directory, choose your original ArcSight Management Center installation directory.
5. 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.)

6. Follow the prompts to complete product initialization.

7. 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**.

You should now upgrade any managed ArcSight Management Centers currently running 2.0 to 2.1 as well.

Migrating from Connector Appliance

Migration is supported from Connector Appliance 6.4 P3 to ArcSight Management Center 2.1 in two steps.

1. Migrate Connector Appliance 6.4 P3 to ArcSight Management Center 2.0. This procedure is described in the Connector Appliance Migration Guide, available on the HP ArcSight support community, Protect724.

2. Upgrade from ArcSight Management Center 2.0 to version 2.1, as outlined above.

Upgrading the ArcMC Agent

ArcSight Management Center 2.1 can only manage nodes that are running the ArcSight Management Center Agent 2.1. Consequently, after upgrading to ArcSight Management Center 2.1, 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

Upgrade Procedure for the ArcMC Agent

ArcSight Management Center 2.1 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 2.1 Administrator's Guide.

Logger Remote Upgrades

This table replaces the one found under "Upgrading a Logger" in the ArcSight Management Center online help file. It describes the remote upgrade scenarios supported by ArcSight Management Center.

Form Factor	Upgrade File Type	Can Upgrade From...	Can Upgrade To...	Comments
Appliance	.enc	Version 6.0 or later	Version 6.1	The filename format for the remote upgrade file for Logger Appliance is `logger-<build number>.enc`
Software	.enc	Version 6.0 or later	Version 6.1	• The filename format for the remote upgrade file for software Logger is `logger-sw-<build number>-remote.enc` • Remote *operating system* upgrade is not supported for software Logger, and, if required, must be performed manually.

Fixed Issues

The following issues have been resolved in ArcSight Management Center 2.1.

Issue	Description
ARCMC-3471	The connector runtime parameter "filter out" display name is now consistent for both connectors and containers.
ARCMC-3274	When running a scheduled SCP backup, the log file would show a cleartext password. The password is now obfuscated.
ARCMC-3200	Previously, the ArcMC monitoring UI would still show "Fatal" when the connector state was changed from down to up. The UI will now show correct status.
ARCMC-3199	Previously, the ArcMC UI showed a connector in a healthy state when the connector was actually down. The correct status will now be shown.
ARCMC-3177	For DNS issues, the timeout period should be set sufficiently so that the user is able to log in. If the issue persists, replace the replace the DNS entry with 0.0.0.0 or another DNS server under /etc/resolv.conf, and then reset the network settings.
ARCMC-2861	The POODLE (Padding Oracle On Downgraded Legacy Encryption) vulnerability (CVE-2014-3566) is resolved.
ARCMC-2860	Whenever the ArcMC Agent is restarted, the status will correctly show as Running.
ARCMC-2857	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-2851	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-2842	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-2837	Prompted pushes will sometimes fail if a subscriber is added to an updated configuration.
ARCMC-2835	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-2834	When a host is relocated from the default location, after rebooting, the host's model and version would previously be reported as Unknown.
ARCMC-2819	Previously an upgrade to a container in FIPS mode would fail. The upgrade will now succeed.
ARCMC-2685	The password of the backup_backup1.xml generated through ArcMC managed logger backup configuration was showing in clear text. The password is now obfuscated.

Issue	Description
ARCMC-2661	The labels on some of the node management columns were shown truncated. Column labels will now be shown correctly.
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-2471	ArcMC will now accept host credential passwords with special characters including: !@#$%^&*()_+.
ARCMC-2218	The ArcMCAgent can now be upgraded on all ArcMC Appliances.
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-2021	On ArcMC appliances, the FTP configuration page will now accept entry of a port range.
ARCMC-1373	On a migrated ArcMC, when setting a value for a Network Configuration, ArcMC will now correctly report changed settings.
ARCMC-304	The navigation tree on the left could sometimes be replaced with the content of the management panel on the right. This issue has been fixed.

Open Issues

ArcSight Management Center 2.1 includes the following open issues. Use listed workarounds, where available.

Issue	Description
ARCMC-4322	After a Logger Pool destination is added to a connector, when attempting to view the details on the Logger pool destination detail page, an error message displayed. Workaround: To view Logger pool destination, do one of the following: -Click Edit Logger Pool Destination to see the details. -In Node Management > Connectors, hover the mouse over the connector to display a tooltip with all Logger pool destination.
ARCMC-4321	In some cases, if a Logger pull destination is configured on a connector, the connector summary page can take a long time to display details.

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-4198	An error(null) can occur if a you upload a Connector AUP to a Connector Appliance 6.4 P3 which is later migrated to ArcMC 2.0 and upgraded to ArcMC 2.1 **Workaround:** - Delete the <versionInProblem> AUP from "upgrade files" repository - SSH to the box - /opt/local/monit/bin/monit stop web - goto /opt/arcsight/userdata/arcmc/repository/upgrade/ folder - delete any leftover .tmp files - Mv all the *<versionInProblem>* connector files to another location - cd /opt/arcsight/userdata/arcmc/repository/upgrade/agents - mv all the *<versionInProblem>* connector files to another location - Make sure no files with <versionInProblem> in their name exist in the opt/arcsight/userdata/arcmc/repository/upgrade/ or in its subfolders - /opt/local/monit/bin/monit start web - Goto UI, re-upload the <versionInProblem> AUP again and emergency restore to that version

Issue	Description
ARCMC-4180	If upgrading from an older ArcMC to newer ArcMC appliance, to use the ArcSight Logger SmartMessage Pool (Encrypted) destination, container upgrade customers need to use SmartConnector release 7.1.5.7534. If using the SmartConnector release 7.1.4.7475 (where ArcSight Logger SmartMessage Pool (Encrypted) is made GA for all customers) perform an "emergency restore" to use the ArcSight Logger SmartMessage Pool (Encrypted) destination feature.
ARCMC-4154	During a push of a Logger initial configuration, the status icon will show In Progress. To show the correct status, click Refresh.
ARCMC-4117	If a host certificate mismatch is reported, the dialog showing the mismatch will erroneously continue to display even if the issue is corrected. To resolve this issue, log out and log back in.
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 10. 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-4022	ArcMC 2.1 cannot be added as a managed host to ArcMC 2.0.
ARCMC-3977	Under Node Management, sorted lists do not save the user-preferred sort order.
ARCMC-3934	During a backup restore operation, if ArcMC is not accessible, manually 'stop' and 'start' all the ArcMC processes via SSH. After the processes restart, wait for the processes to be up and running. An explanation of stop, start, summary/status command is available in the Admin guide.

Issue	Description
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-3862	In some circumstances, after creating a search group on a Logger, importing it to a second Logger, and then pushing the group to a destination Logger, the search group is incorrectly categorized as Shared on the destination Logger.
ARCMC-3732	On the node management tab, the title bar may be shown broadly. This is a cosmetic issue only.
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-3563	If the storage volume on a managed Logger is not set, then peering, initial configuration, and the license entitlement report will not function correctly for the Logger.
ARCMC-3514	The Monitoring Summary can show duplicated connector type names.
ARCMC-3086	Immediately after installation, in some cases, the following message is displayed: "The requested URL's length exceeds the capacity limit for this server." If this message displays, please exit and relogin, or refresh the browser.
ARCMC-2969	Context sensitive help for the All Configurations and Repositories menu items will not show the correct help.
ARCMC-2855	The /etc/hosts file is not restored from backup after a restore. **Workaround**: On the **System Admin > Network > Host** tab, re-edit the content after the restore operation.
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 empty string causes issues with the DNS provider.
ARCMC-2420	In some cases, while uploading an ENC file, although the upgrade completes, the upgrade status on the License and Upgrade page still shows as installing. If this occurs, wait at least 40 minutes and then refresh the browser.
ARCMC-1284	If an attempt is made to add a CEF encrypted syslog destination using the Choose from an 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, use only the Create a New Destination option.
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. 1. Click **Setup > System Admin > Process Status.** 2. From the list of connectors, select the connector to restart and then click the **Restart** button.

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 2.1)

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@hp.com.

We appreciate your feedback!