Release Notes
ArcSight Connector Appliance

Version 6.4 Patch 1

June 1, 2013

ArcSight
An HP Company

Revision History

Date	Product Version	Description
06/01/13	6.4 Patch 1	Adds support for HP ProLiant G8 servers and a new factory restore process for these servers.
11/10/12	6.4 GA	Updated the features list, added instruction for Software Connector Appliance upgrades and updated open/closed issues.
07/11/12	6.3 GA	Added note for CheckPoint SmartConnector users.
01/17/12	6.2 Patch 1	Updated the upgrade process to include a means of preserving management configuration data when upgrading from 6.2 to 6.2, Patch 1.
11/16/11	6.2 Patch 1	Added time zone information and fixed issues.
09/12/11	6.2 GA	Added new feature list, updated upgrade procedure, and added open/closed issues.
05/13/11	6.1 GA	Added new feature list, updated upgrade procedure, and added open/closed issues.
09/20/10	6.0 GA	Updated upgrade procedure, and added open/closed issues.
08/13/10	6.0 Beta	Added new feature list, updated upgrade procedure, and added open/closed issues.

Document template version: 2.1.1

Contact Information

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

Contents

Release Notes

These release notes provide information about ArcSight Connector Appliance 6.4 Patch 1 (Build C6820) and is strictly for users using the new Connector Appliance hardware platforms, **C3500** and **C5500**.

This patch does not support upgrades, and should not be used to upgrade existing installations.

This document discusses the following topics:

What's New in Connector Appliance 6.4 Patch 1

The Connector Appliance 6.4 Patch 1 release provides the same functionality as Connector Appliance 6.4 GA. However, this release is designed to run on the new Connector Appliance hardware platforms available from HP. The following enhancements were introduced in this release:

- **New Hardware Platform Support.** This release is designed to run on the new Connector Appliance hardware platforms, **C3500** and **C5500**, which are based on the HP ProLiant G8 series.
- **New Factory Restore Process.** A new, simplified factory restore process is available for the new hardware platforms. See "Factory Restore Process for C3500 and C5500" on page 9 for details. The process to restore the previous models (Cx400 and earlier) remains the same and is documented in the *Connector Appliance 6.4 Administrator's Guide*.
- **Enhanced Size for SSL Certificates.** The key size of the pre-installed, self-signed SSL certificate that Connector Appliance presents to HTTPS clients is now 2048 bits. Previously, the key size was 1024 bits.
- **Expanded FTP directory size.** The new hardware platforms support a maximum FTP directory size of 500 GB. The following table lists all models (including the new models) and their maximum directory size.

Model Name	Maximum Directory Size (GB)
C1300	95
C1400	275
C3200	285
C3400	275
C3500	**500**
C5200	240
C5400	235
C5500	**500**

- **Backup and Restore.** A backup created on an existing Connector Appliance model can be restored to the equivalent new hardware model. Therefore, a backup created on C3200 or C3400 can be restored to C3500; similarly, a backup created on C5200 or C5400 can be restored to C5500.

Supported Browsers

For this release, these browser versions are supported for accessing the Connector Appliance user interface:

Microsoft Internet Explorer: Versions **8.0** and **9.0**

Mozilla Firefox: Versions **16.0** and **17.0**

Supported SmartConnectors

The list of SmartConnectors available in the **Connector Type** pull-down menu includes all supported SmartConnectors. Some SmartConnectors are not currently supported for use on the Connector Appliance, but can be managed remotely. For the current list of SmartConnectors that Connector Appliance can manage, including those that require additional setup, search for the knowledge base the article *Supported SmartConnectors for Connector Appliance* available under the Self-solve tab of the HP SSO site at http://support.openview.hp.com/.

Syslog and SNMP SmartConnectors

You can install all syslog and SNMP SmartConnectors on the Connector Appliance.

To prevent performance degradation, ArcSight strongly recommends that you do not have more than one syslog connector in a container. For more information, search for the article *Running more than one syslog connector in one container* available under the Self-solve tab of the HP SSO site at http://support.openview.hp.com/.

Database Type SmartConnectors

You can run database SmartConnectors that connect to Windows-based databases (such as Microsoft SQL Audit DB) on Linux or other platforms using JDBC drivers. The *ArcSight Connector Appliance Administrator's Guide* describes how to obtain and install the required JDBC drivers, and how to use the user-defined JDBC Repository feature to install the drivers on the local Connector Appliance.

Database connectors that use Microsoft SQL Server 2005 JDBC Driver **1.2** do not run in FIPS mode. For the database connectors to run in FIPS mode, you need to install Microsoft SQL Server 2005 JDBC Driver **1.1**.

File-Based SmartConnectors

Any event sources, including scanners running in automatic mode and Windows-based sources, can write to files on a Remote File System that the Connector Appliance can mount and access. Connector Appliances supports CIFS and NFS shares.

All file-based SmartConnectors require CIFS or NFS storage mounts ***before*** configuring the SmartConnector.

From Connector Appliance, do the following to configure a **CIFS mount**:

Setup > **System Admin** > **Storage**> **Remote File System** > **Add** > **CIFS**

OR the following to configure a **NFS mount**:

Setup > **System Admin** > **Storage** > **Remote File System** > **Add** > **NFS**

For more information, see the *ArcSight Connector Appliance Administrator's Guide*.

API Type SmartConnectors

On the Connector Appliance, you cannot use Microsoft and other API-type SmartConnectors that need to be located on the host they are monitoring.

CheckPoint OPSEC SmartConnectors are supported in `sslca` mode using the `pull cert` command described in the *ArcSight Connector Appliance Administrator's Guide*.

The following API-type SmartConnectors work with the Connector Appliance, but with the limitations listed below.

API SmartConnector	Limitation
Check Point FW-1/VPN-1 OPSEC	Only clear channel and `sslca` are supported. `sslopsec` is not supported.
Check Point FW-1/VPN-1 OPSEC (Legacy)	Only clear channel and `sslca` are supported. `sslopsec` is not supported.
Sourcefire Defense Center eStreamer	Not supported in FIPS mode.
Windows Unified	Not supported in FIPS mode.

Kernel Warning Message on Bootup

The following message is displayed during the initial startup screen of Red Hat Linux on Logger L3500, L7500, and L7500-SAN appliances:

```
[Firmware Bug]: the BIOS has corrupted hw-PMU resources
```

A similar message is posted to the `dmesg` file.

These messages do not affect the functionality or performance of the operating system or the server and can be safely ignored. For more information, refer to the HP Customer Advisory document at:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03265132&lang=en&cc=us&taskId=101&prodSeriesId=4268690&prodTypeId=3709945

Upgrade Information

Upgrading to Connector Appliance 6.4 Patch 1

Since Connector Appliance version 6.4 Patch 1 is a hardware-centric release, an upgrade of existing installations to this release is **not** supported.

Upgrading Containers

Upgrading containers residing on the new Connector Appliance hardware platforms, C3500 and C5500, to SmartConnector build 6.0.1.6574 is not supported. Therefore, **do not upgrade to SmartConnector build 6.0.1.6574**. Instead, upgrade to the latest available SmartConnector build subsequent to 6.0.1.6574.

Factory Restore Process for C3500 and C5500

The process to restore factory settings for the new models is different than the previous (Cx400 and earlier) models.

> **Note**
>
> The instructions in this section are for the new factory restore process.
>
> If you need to restore factory settings on your existing (Cx400 or earlier) Connector Appliance, follow the instructions in the *Connector Appliance 6.4 GA Administrator's Guide*.

Restoring the CX500

You can restore CX500 appliances to the original factory settings by using the built-in System Restore utility.

To restore an CX500 appliance:

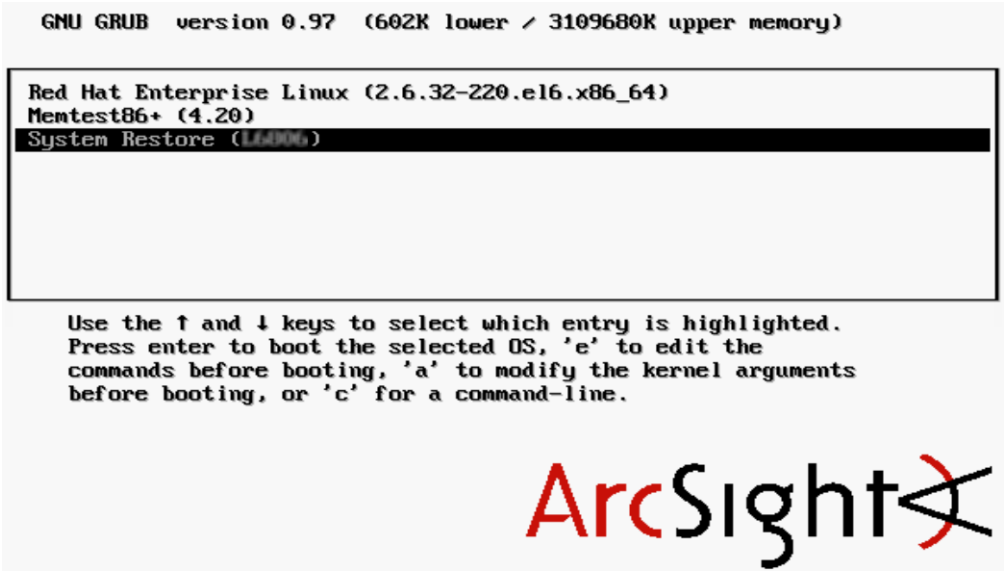
1. Attach a keyboard, monitor, and mouse directly to the appliance, or if your appliance is configured for remote access through iLO, you can use that functionality to access the appliance console.
2. Log into the appliance. Type `reboot` at the command prompt, and then press **Enter**.

   As the system reboots, messages scroll by. As soon as a message like the following appears on the screen, press any key on your keyboard.

   ```
   Press any key to enter the menu
   Booting Red Hat Enterprise Linux <version> in N seconds...
   ```

   > **Note**
   >
   > This message is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance will continue to boot normally.

3. The GNU GRUB window opens, as shown in the example below.



Use the mouse or arrow keys to select **System Restore CXXXX**, where XXXX represents a four-digit appliance build number, and press **Enter**.

4. System Restore automatically detects and displays the archive image. The image is named following the pattern `YYYY-MM-DD_CX500_C<XXXX>.ari`, where `YYYY-MM-DD` is the date, `CX500` is the appliance version and `CXXXX` is the appliance build number.
5. Press **F1** (AUTOSELECT) to automatically map the Source Image, displayed in the top panel, to the Target Disk, displayed in the bottom panel. The restore image name is displayed in the right-most column.
6. Optionally, press **F10** (VERIFY) to check the archive for damage before performing the restore. Once the archive has been verified, press **Enter** to continue.
7. Press **F2** (RESTORE) to begin the restore process. A dialog box asks whether you want to restore. Press **y** to proceed with the restore or **n** to cancel.
8. Progress bars show the status of the restoration.

Do not interrupt or power-down the appliance during the restore process. Interrupting the restore process may force the system into a state from which it cannot be recovered.

When the restore process is complete, press F12 to reboot the appliance. A dialog box asks whether you want to reboot. Press **y** to proceed with the reboot.

Doc Errata

Note the following errors in the Connector Appliance 6.4 GA Administrator's Guide. These errors will be corrected during the next update of the guide.

- There are instances within the *Connector Appliance 6.4 GA Administrator's Guide* where the directory path `opt/arcsight/container_name/...` or `opt/arcsight/connector_x/...` appear. In such instances, replace `opt/arcsight` with `opt/arcsight/connectors`. The rest of the path should remain as is.
- Additionally, the following statement in the *Connector Appliance 6.4 GA Administrator's Guide* is incorrect:

  "Connector Appliance cannot remotely manage connectors running on AIX."

  The correct statement should be:

  "Connector Appliance **can** remotely manage connectors running on AIX."

- The following audit events are missing from the list of Platform Events in the *Connector Appliance 6.4 GA Administrator's Guide*.

Signature	Severity	Definition	Category
platform:242	5	Removed all members from group	/Platform/Authorization/Groups/Membership/Update/Clear
platform:249	7	Account Locked	/Platform/Authentication/AccountLocked

Signature	Severity	Definition	Category
platform:409	3	Configure login warning banner	/Platform/Configuration /LoginBanner

Fixed Issues

The following issues have been resolved in this release.

Issue	Description
CONAPP-4220	If a container was in FIPS mode, it could not be upgraded from SmartConnector release 5.2.5 to 5.2.6.
CONAPP-4143	If a Connector Appliance ran low on memory (when a large number of containers were being managed, for example), the EPS gauges at the top of the Monitor Summary page would not update or show accurate values.
CONAPP-3808	When creating a CIFS mount on Windows 2008 R2 servers, the "sec=ntlmv2i" mount option caused "mount error 22 = Invalid argument" error in /var/log/messages. FIX: When creating a CIFS mount on a Windows 2008 R2 server configured to enforce NTLMv2 authentication and packet signing, use the option "sec=ntlmsspi" instead of "sec=ntlmv2i" in the CIFS mount command, or install Microsoft hotfix KB957441 on the Windows server.

Open Issues

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

Issue	Description
CONAPP-4424	All G8 host are showing model and version unknown.
CONAPP-4162	Subdirectories are not backed up during the backup process. Therefore, when a configuration is restored from a backup, the FTP subdirectories are not restored. Workaround: Manually add the FTP sub-directories after restoring a configuration.
CONAPP-4161	If you update the year portion of the date manually, using the Connector Appliance GUI, the changes do not take effect. Workaround: Change the entire date, and not just the year.
CONAPP-4132	On the IE browser, the Hosts file (System > Network > Hosts) loses formatting when it is imported using the Import from Local File button. Workaround: When using the IE browser, copy and paste the Hosts file from a text editor such as Notepad to preserve formatting instead of using the Import from Local File button.

Issue	Description
CONAPP-4100	ArcExchange displayed the following authentication error: "The code can't reach Protect724.arcsight.com" Understanding: This issue occurs if there is a proxy used to get to Protect724 ArcSight Community.
CONAPP-4069	On an L3200 (integrated Logger-Connector Appliance platform), enabling or disabling FIPS might fail. Understanding: This issue is specific to older generation of appliances and is not observed on the HP Proliant-based models.
CONAPP-4057	When a connector is upgraded to version 5.2.6.6434.0, the default SNMP PDU fields are not available on the connector when an SNMP destination is configured using this connector. Workaround: Use the Emergency Restore process to restore the container to 5.2.6.6436.0 version; SNMP PDU fields are available in this version.
CONAPP-3747	The configuration backup fails when either the connector or repository data grows too large. Workaround: Retrieve the configuration by excluding the connector and/or repository data.
CONAPP-2691	If there are two SmartConnectors sharing the same container and the same destination, the framework combines the two EPS OUT stats values. As a result, the UI displays 0 for the first connector and the combined EPS values for the second. There is no data loss when this occurs.
CONAPP-742 TTP#50651	All of the Monitor pages show incorrect dates. Workaround: Restart the web process to fix the issue.