Release Notes
ArcSight™ Connector Appliance

Version 6.3 GA (Build C6386)

July 11, 2012

ArcSight™
An HP Company

Release Notes ArcSight™ Connector Appliance, Version 6.3 GA (Build C6386)

Revision History

Date	Product Version	Description
07/11/12	6.3 GA	Added note for CheckPoint SmartConnector users.
04/24/12	6.3 GA	Added new feature list and updated open/closed issues.

Release Notes template version: 2.0.0

ArcSight Customer Support

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 ArcSight Connector Appliance v6.3 GA 5

What's New in Connector Appliance v6.3 GA 5
Licensing 6
Supported Browsers 6
Upgrading to v6.3 GA 6
Upgrade Files 7
Upgrading Connector Appliance 7
Upgrade Information You Need to Know 8
General Information You Need to Know 9
Port Change for HTTP Requests 9
Upgrading to the Latest SmartConnector Version 9
Supported SmartConnectors 10
Syslog and SNMP SmartConnectors 10
Database Type SmartConnectors 10
File Type SmartConnectors 10
API Type SmartConnectors 11
Closed Issues 11
Open Issues 11

Release Notes
ArcSight Connector Appliance v6.3 GA

The Connector Appliance is a hardware and software solution that manages local and remote ArcSight SmartConnectors. SmartConnectors gather network security and other events, and send processed events to various destinations, including ArcSight ESM and ArcSight Logger.

Connector Appliance 6.3 GA is the first release available in two form factors: the existing hardware-based Connector Appliance and a new software version of Connector Appliance, which can be installed on any supported platform. The software version of Connector Appliance offers users much of the functionality of Connector Appliance with the flexibility to use their own hardware. The software version does not contain local SmartConnectors, but does provide full management control.

These release notes provide information about the ArcSight Connector Appliance v6.3 GA (C6386) release. Read the entire document before installing or upgrading to this release.

This document discusses the following topics.

- "What's New in Connector Appliance v6.3 GA" on page 5
- "Supported Browsers" on page 6
- "Upgrading to v6.3 GA" on page 6
- "Upgrade Information You Need to Know" on page 8
- "General Information You Need to Know" on page 9
- "Closed Issues" on page 11
- "Open Issues" on page 11

What's New in Connector Appliance v6.3 GA

ArcSight introduces the following new features and enhancements for Connector Appliance v6.3 GA.

- **Scheduled Configuration Backup.** Provides the ability for users to schedule their configuration backups.
- **Software version of Connector Appliance.** Offers users much of the functionality of Connector Appliance with the flexibility of using their own hardware.
- **LDAPS.** Now offers support for authentication using LDAP over SSL.
- **Simplified ability to change SNMP Community String.** SNMP options can be easily updated through the UI, rather than the Diagnostics Tools menu. *(Appliance only)*
- **IP Aliasing.** Users can create aliases for their listed NICs. *(Appliance only)*

- **Expanded Diagnostic Tool functionality.** Now includes a display of I/O statistics and an option for listing open files. *(Appliance only)*
- **Simplified Authentication options.** Offers an updated and expanded set of authentication settings.
- **Updated User Management.** Users have five new attribute options.
- **Backup for RADIUS.** Now allows for failover to a backup RADIUS server.

To successfully use local **Checkpoint SmartConnectors** on a new HP Connector Appliance shipped with version 6.3, users must first upgrade the appropriate container to **SmartConnector 5.2.4 (Build 6326)**.

Licensing

To initiate license procurement, follow the instructions in the emailed Electronic Delivery Receipt (EDR) you received from HP after placing your order.

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 **7.0** and **8.0**

When a Connector Appliance page fails to load correctly or appears blank, try clearing the browser cache.

To do so, in

- **Internet Explorer**: Navigate to **Tools** > **Internet Options**, then, under **Browsing history,** click the **Delete** button.
- **Firefox 7.0**: From the **Tools** menu, choose **Clear Recent History**.
- **Firefox 8.0**: From the **Tools** menu, choose **Options > Clear Now**.

An **Adobe Flash Player** plug-in is required on these browsers for some of the features, such as EPS gauges, to work.

Upgrading to v6.3 GA

You can upgrade to Connector Appliance v6.3 GA from Connector Appliance v6.2 GA or v6.2, Patch 1. Additionally, the **C1000**, **C3000**, and **C5000** appliances cannot be upgraded to this release.

To determine your current Connector Appliance version, hover the mouse over the ArcSight logo in the upper left of the screen. You can also click **Setup** > **System Admin** > **License & Update** and look for the `arcsight-appliance` component.

Upgrade Files

These files are available from the HP SSO site at http://support.openview.hp.com/:

- `appliance-6386.enc`

  Use this file to upgrade the local Connector Appliance (localhost) to v6.3 GA.

- `ArcSight-6.3.0.6386.0-ConnectorAppliance.full.aup`

  Use this file to upgrade remotely-managed Connector Appliances from a central appliance. Follow the instructions for upgrading a host in the *ArcSight Connector Appliance Administrator's Guide*.

Upgrading Connector Appliance

You need to upgrade the local appliance (localhost) with the `appliance-6386.enc` file before you can upgrade remotely-managed appliances.

Upgrading to v6.3 GA on a Locally Managed Connector Appliance

1. Reboot the Connector Appliance.
2. From the HP SSO site (http://support.openview.hp.com/), download the `appliance-6386.enc` file to the computer that you use to connect to the Connector Appliance interface.
3. From the computer to which you downloaded the upgrade file, log in to the Connector Appliance browser-based interface using an account with administrator (upgrade) privileges.
4. Click the **Setup** > **System Admin** tab.
5. From the **System menu** in the left panel, click **License & Update**.
6. To locate the upgrade file you downloaded in Step 2, click **Browse**.
7. Click **Upload Update**.
8. Click **OK**.
9. The End-User License Agreement appears. Review and scroll down and check the **I Accept the terms and License Agreement** box.
10. The login box appears. Log back in.
11. Click the **Reboot** link.
12. Click the **Start Reboot Now** button.
13. After the reboot is complete, the End-User License Agreement page appears. Review and scroll down and check the **I Accept the terms and License Agreement** box.
14. Login to the Connector Appliance.
15. Go to **Setup** > **System Admin > License & Update** and confirm that the Connector Appliance is running v6.3 GA (6.3.0-C6386).

Upgrading to v6.3 on a Remotely Managed Connector Appliance

1. Make sure that all of your remotely managed Connector Appliances are running v6.2 GA (C6244) or v6.2 Patch1 (C6261).

To determine the version of your remote appliances, click the **Manage** tab. Find the Host under **System** in the left side panel and click to view it's main page. The main page lists all of the remotely managed hosts. The current version is listed in the **Version** column.

2. From Connector Appliance user interface, click **Setup > Repositories** from the top-level menu bar.
3. Click **Upgrade AUP** from the left panel.
4. Click **Upload**.
5. Click **Browse** to select the `ArcSight-6.3.0.6386.0-ConnectorAppliance.full.aup` file from your local computer.
6. Click **Submit**.
7. Once complete, click the **Manage** tab.
8. Select the **Hosts** tab in the right panel, then select the appliance to which you want to apply the patch.
9. Click **Upgrade**.
10. From the drop-down list, select `ArcSight-6.3.0.6386.0-ConnectorAppliance.full.aup` and follow the wizard.

Upgrade Information You Need to Know

The following provides tips that can help you troubleshoot issues you might encounter when upgrading Connector Appliance containers.

When upgrading an empty container, the upgrade fails.

To upgrade a container on Connector Appliance that does not contain any connectors, perform an Emergency Restore operation to install SmartConnector `build 5.2.2.6221`. This is a one-time operation. After upgrading to SmartConnector `build 5.2.2.6221`, you can directly upgrade empty containers to the newer versions without having to perform Emergency Restore.

For detailed instructions on using the Emergency Restore feature, refer to the *Connector Appliance Administrator's Guide*.

Unable to upgrade a Connector Appliance container when upgrading to the 5.1.3 SmartConnector release.

From the left panel, do the following:

1. Upgrade AUP to upload the 5.1.4 AUP to the Connector Appliance repositories.
2. Back up files to backup all of the configuration files for the relevant container.
3. Use Emergency Restore on the same container by selecting the 5.1.4 AUP from the drop-down menu.
4. Apply the backup to the container by pushing the files created earlier.

If you want to upgrade the container using a SmartConnector release prior to 5.1.3, upgrade directly to connector release 5.1.4, not the 5.1.3 release. If you still are unable to upgrade, perform the steps listed above.

A temporary connector is created when an empty container on Connector Appliance is upgraded from v5.1.2 to v5.1.4.

To avoid having a temporary connector when upgrading, perform an Emergency Restore operation to install SmartConnector `build 5.2.2.6221`. This is a one-time operation. After upgrading to SmartConnector `build 5.2.2.6221`, you can directly upgrade empty containers to the newer versions without having to perform Emergency Restore.

For detailed instructions on using the Emergency Restore feature, refer to the *Connector Appliance Administrator's Guide*.

General Information You Need to Know

This section highlights important Connector Appliance information.

Port Change for HTTP Requests

Connector Appliance now redirects HTTP requests for port 80 to port 443 so that you can access the Connector Appliance login page by typing just the appliance hostname or IP address into the browser address field.

This does not apply to the software version of Connector Appliance.

If you are using port 80 on your SmartConnectors, reconfigure the connectors to use a different port before you upgrade Connector Appliance.

Upgrading to the Latest SmartConnector Version

All instruction for upgrading SmartConnectors pertains to the hardware-based version of Connector Appliance.

To upgrade the connectors you manage on the Connector Appliance to the latest SmartConnector version, you need to apply the latest build to the container that contains those connectors. For information about upgrading a container to a specific connector version, refer to the *ArcSight Connector Appliance Administrator's Guide*.

Supported SmartConnectors

The list of SmartConnectors available in the Connector Type pull-down 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 supported for installation on Connector Appliance, including those that require additional setup, refer to the article *Supported Products for Connector Appliance*

from the ArcSight Knowledge Base. To access the Knowledge Base, search 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, refer to the article *Running more than one syslog connector in one container* from the ArcSight Knowledge Base.

To access the Knowledge Base, search 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 Type SmartConnectors

Any event sources, including scanners running in automatic mode and Windows-based sources, can write to files on a Remote File System (also known as NFS and CIFS Storage) that the Connector Appliance can mount and access.

Appliance-based, file-type SmartConnectors require NFS or CIFS storage mounts, as appropriate. Configure an NFS mount (**Setup** > **System Admin** > **Storage** > **Remote File System** > **Add** > **NFS**) or a CIFS mount (**Setup** > **System Admin** > **Storage**> **Remote File System** > **Add** > **CIFS**) before configuring the SmartConnector. 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.

API SmartConnector	Limitation
Sourcefire Defense Center eStreamer	Not supported in FIPS mode.
Windows Unified	Not supported in FIPS mode.

Closed Issues

The following issues have been resolved in this release.

Issue	Description
CONAPP-3723	Documentation was required stating that when mounting a CIFS share for a windows 2008 cluster, a hostname rather than an IP must be used. Fix: This information has been added to the "Connector Appliance Administrator's Guide".
CONAPP-3595	The message that appeared when an authentication failure occurred on Connector Appliance could lead to a security vulnerability. Fix: The message has been updated to remedy the situation.

Open Issues

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

Issue	Description
CONAPP-3768	In Internet Explorer 8 and 9, the "Save" button and the "Restart Network Service" link under Setup => Sytem Admin => Network => System DNS are almost off screen when the page is first loaded, but once the browser is resized, the button and link disappear altogether. Workaround: Reload or refresh the page.
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.

Issue	Description
CONAPP-3721	If a user running client authentication does a backup, then attempts to restore their configuration, users cannot successfully login using CAC authentication. The login screen shows "Invalid Certificate". Workaround: 1. Login as the default admin user. 2. Go to Setup => System Admin => Authentication => External Authentication 3. From the drop down list for Authentication Method, change it from Client Certificate to Local Password. 4. Click Save. 5. On the Pop-up "This change requires a restart of the web server. Are you sure you want to restart the web server?", click Yes. 6. From the Pop-up, "Configuration saved successfully. Remember to configure Local Password settings separately" click OK. 7. From the drop down list for Authentication Method, change it from Local Password back to Client Certificate. 8. Click Save. 9. On the Pop-up "This change requires a restart of the web server. Are you sure you want to restart the web server?" click Yes. 10. On the Pop-up "Configuration saved successfully. Remember to configure Local Password settings separately" click OK. 11. Upon logging out, Client Certificate authentication should be successful.
CONAPP-3719	The CLI login does not support LDAPS. If LDAPS is configured, a user with a DN configured falls back to local password for the CLI login. For users that do not have a DN configured, the login fails.
CONAPP-3699	Host AUP upgrade is not working. The issue is reproduced only if the Connector Appliance version is 6.0 or lower and Container 1 on the slave Connector Appliance is not on build 5.1.1 or lower. Workaround: Log in to the remote Connector Appliance and upgrade to version 6.1, then follow the supported upgrade paths using the enc file. After the process is complete, users can upgrade remotely using AUP.
CONAPP-3614	Software version: If a user creates an empty folder prior to installation and chooses that empty folder for their installation, then executes the uninstaller, the uninstaller will delete the created folder.
CONAPP-3343	If an upgrade fails, the UI might show the container as running the new version, but after a reboot appears to be running the previous one. When the failure occurs and the upgrade is rolled back, but the process for the "new" version is not killed until the next reboot.
CONAPP-3249	Multiple copies of the same Content AUP file is created in the user/agent/aup directory. This causes large "Appliance Backup" files to accumulate.
CONAPP-3094	When applying an appliance backup, SSL Server certificate, FTP, and container version information failed to carry over. Workaround: Manually recreate these settings in the restored appliance.
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.

Issue	Description
CONAPP-2655	After backing up and restoring the Connector Appliance, the CIFS mount is unavailable. Workaround: Edit the CIFS mount (Setup > System Admin > Remote File Systems > check the CIFS mount > Edit), then re-enter the username and password.
CONAPP-2598	If you are running a connector in FIPS mode and try to add the ArcSight Logger SmartMessage (encrypted) destination, a warning message appears stating that the connection to the destination has failed a ping test. This occurs even if all the destination parameters are correct and the SSL certificate for the Logger appliance is correctly imported into the connector trust store.