Release Notes
ArcSight™ Connector Appliance

Version 6.2 GA (Build C6244)

January 17, 2012

ArcSight™
An HP Company

Release Notes ArcSight™ Connector Appliance Version 6.2 GA (Build C6244)

Revision History

Date	Product Version	Description
01/17/12	6.2 GA	Updated the upgrade process to include a means of preserving management configuration data when upgrading from 6.1 to 6.2.
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

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 v6.2 GA

The Connector Appliance is a hardware 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.

These release notes provide information about the ArcSight Connector Appliance v6.2 GA (C6244) release. Read the entire document before installing this release.

This document discusses the following topics.

What's New in Connector Appliance v6.2 GA

ArcSight introduces the following new features and enhancements for Connector Appliance v6.2 GA.

- **Appliance Health and Performance Monitoring** – The SNMPv2 MIB supports any SNMP-enabled network application to monitor Connector Appliance health and performance.
- **LDAP/Active Directory User Authentication** – A Connector Appliance user can now be authenticated through LDAP/Active Directory.
- **Read-Only User Group** – New read-only user groups are available for administrators to control access to and operation of the Connector Appliance. Users in the read-only user group can view appliance and connector configuration settings, but cannot make modifications to them.
- **SSL Server Certificate Expiration Notification** – The Connector Appliance can generate an expiration alert for an SSL server certificate before it expires.
- **Automatic Password Reset** – Once their email notification setting is properly configured, any Connector Appliance user can reset their forgotten password.
- **Bulk Certificate Import** – ArcSight users can now conduct bulk downloads of destination certificates from ESM and bulk import them into any SmartConnector.
- **Login Banner Customization** – The Connector Appliance user interface has been enhanced to allow and support user customization of the login banner.
- **FTP Enabled for BlueCoat SmartConnector** – Connector Appliance allows for FTP enabled events file processing in support of the BlueCoat Proxy SG Multi-File SmartConnector.
- **Windows CIFS Operation Improvement** – The Connector Appliance can now provide better operation support under Microsoft Windows network environment.
  - **Microsoft NTLMv2 Support** – The Connector Appliance supports the Microsoft NTLMv2 authentication.
  - **UNC Path Naming** – The Connector Appliance supports CIFS mounts using Microsoft Windows Uniform Naming Convention (UNC) or naming notation.
- **New SmartConnector Support** – The Connector Appliance can now support versions of both **Microsoft Forefront Threat Management Gateway File** and **Microsoft Network Policy Server File** SmartConnectors via the latest SmartConnector release.
- **Latest SmartConnector Release Bundle** – This release provides bundled versions of the most up-to-date, new and updated ArcSight SmartConnectors.

Supported Browsers

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

Microsoft Internet Explorer: Versions **8.0** (certified) and **9.0** (certified)

Mozilla Firefox: Versions **3.6** (certified) and **6.0** (supported)

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**: From the **Tools** menu, choose **Clear Recent History**.

Upgrading to v6.2 GA

You can upgrade to Connector Appliance v6.2 GA from Connector Appliance v6.1. Take care that you sequentially perform each of the steps in the following three sections.

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.

When upgrading from **Connector Appliance v6.1 to v6.2**, there is a possibility that your current location and host configurations may be lost in the upgrade. To prevent this, see “Preserving Your Remote Management Configuration” on page 8.

When upgrading to Connector Appliance v6.2,

- Custom groups created in previous versions will be carried over to the new version, but any rights introduced in 6.2 (such as “view management” rights) **will not** be automatically enabled. The administrator must enable these rights after the upgrade is complete.
- Option rights **will not** be automatically enabled. The administrator must enable these rights after the upgrade is complete.

Upgrading Files

Before beginning the upgrade, verify your current remote management configuration (your location, host and connector information), then export the data before starting the upgrade process. If you have not already performed this step, see “Preserving Your Remote Management Configuration” on page 8 for instructions.

The following files are available from the ArcSight Customer Support download site at https://arcsight.subscribenet.com

- `appliance-6244.enc`

  Use this file to upgrade the local Connector Appliance (localhost) to v6.2 GA.

- `ArcSight-6.2.0.6244.0-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*.

> **Caution** On a **C3000** appliance, upgrading remote Connector Appliances using an `.aup` file might fail if not enough memory for the web process is present.
>
> To prevent failure, upgrade the remote Connector Appliances locally using an .enc file.

Preserving Your Remote Management Configuration

ArcSight recommends that you export your remote management configuration before upgrading. If performing an upgrade on any remote Connector Appliances, **you must login directly to the remotely-managed appliance before performing the steps that follow**.

To export your remote management configuration, do the following:

1. Click **Manage** from the top-level menu bar.

   The **Location** tab displays as the default page.

2. From under the **Location** tab, click the **Export Remote Configuration** icon.

3. Click **Next** within the **Export Remotely Managed Hosts** Wizard to export the repository.

   This exports the Remote Management Config AUP file and places it into the **Remote Management AUP Repository**.

4. Click the **Remote Management AUP** link to access the **Remote Management AUP Repository**.

5. From within the **Last Modified** column, locate the newly exported Remote Management Config AUP file within the **Remote Management AUP Repository** then use the **Retrieve** icon to save it to another location.

6. Perform the version 6.1 to 6.2 upgrade. See Upgrading Connector Appliance below for instructions.

Upgrading Connector Appliance

Note

You need to upgrade the local appliance (localhost) with the `appliance-6244.enc` file before you can upgrade remotely-managed appliances.

To upgrade Connector Appliance to v6.2 GA

1. Verify your current remote management configuration (your location, host and connector information), then export the data before starting the upgrade process. If you have not already performed this step, see "Preserving Your Remote Management Configuration" on page 8 for instructions.
2. Reboot the Connector Appliance.
3. From the ArcSight Customer Support download site (https://arcsight.subscribenet.com), download the `appliance-6244.enc` file to the computer that you use to connect to the Connector Appliance interface.
4. 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.
5. Click the **Setup** > **System Admin** tab.
6. From the **System menu** in the left panel, click **License & Update**.
7. To locate the upgrade file you downloaded in Step 3, click **Browse**.
8. Click **Upload Update**.
9. When the upload completes and the reboot message appears, reboot the Connector Appliance.
10. Go to **Setup** > **System Admin > License & Update** and confirm that the Connector Appliance is running v6.2 GA (6.2.0-C6244).

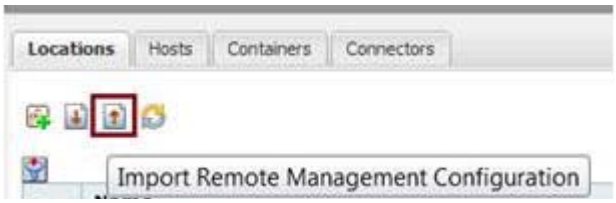
Note

If using an AUP to upgrade any remote Connector Appliances, you must login directly to the remotely-managed appliance before performing the steps that follow.

11. Click **Manage** from the top-level menu bar. If your previous configuration appears in the left panel, the upgrade is complete.

    If you **do not** see your previous configuration in the left panel, you can restore your previous configuration by importing the Remote Management Config AUP file you saved in Step 1 of this process. To start,

    a. From the **Locations** tab, use the **Import** icon to launch the import wizard to restore your previous configuration, as shown below.



    b. Click **Next** within the **Import Remote Management Configuration** Wizard.

c Choose **Full remote management (AUP format)**, then click **Next**.

d Click **Upload** to browse for the previously saved Remote Management Config AUP file, then click **Submit**.

Information You Need to Know

This section highlights important Connector Appliance information.

Remote Management AUP Importing

When importing a remote management AUP for remotely managed hosts onto an appliance, you may see an error message that states “Wrong appliance model in remote management AUP file”. If this occurs, upgrade the appliance to version 6.2.

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.

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

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, go to the ArcSight Support Center web page, click the Knowledge Base link, and log in.

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.

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** > **NFS**) or a CIFS mount (**Setup** > **System Admin** > **Storage**> **Remote File System** > **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.
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-2724	Was unable to delete a user that was currently logged in or had logged out recently.
CONAPP-2675	Creating multiple WUC connectors in one container caused the connectors to hang and not process events.
CONAPP-2624	The ESM certificate automatic download feature did not support failover destinations.

Issue	Description
CONAPP-2604 TTP#49855	When making changes to default settings on ESM, the destination-specific configuration settings on the Connector Appliance were overwritten.
CONAPP-1999 TTP#68340	RAID and Sensor internal events were not generated.
CONAPP-946 TTP#54674	The Connector Appliance user interface did not support user customization of the login banner.
CONAPP-217 TTP#43643	When a configuration backup failed during restore, the wrong window displayed, resulting in nested frames.
CONAPP-194 TTP#43480	URLs for the Connector Appliance showed Logger.

Open Issues

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

Issue	Description
CONAPP-3139	When upgraded to the 5.1.3 SmartConnector release, you are unable to upgrade a Connector Appliance container. Workaround: From the left panel, use 1. Upgrade AUP to upload the 5.1.4 AUP to the Connector Appliance repositories. 2. Backup files to back up all of the configuration files for the relevant container. 3. Emergency Restore on the same container by selecting the 5.1.4 AUP from the drop-down menu. 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 release 5.1.3. If you still are unable to upgrade, perform the steps listed above.
CONAPP-3094	When applying an appliance backup, SSL Server certificate, SSL client authentication, FTP, and container version information fail to carry over. Workaround: Manually recreate these settings in the restored appliance.
CONAPP-2734	If you reboot the appliance, log back in to Connector Appliance, then click the Setup > System Admin menu, occasionally, the ArcSight Logger Login page on displays. Workaround: Wait approximately three minutes after the system reboots before logging back in to Connector 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.
CONAPP-2655	After backing up and restoring the Connector Appliance, the CIFS mount is unavailable. Workaround: Edit the CIFS mount (Setup > System Admin > CIFS), then re-enter the username and password.

Issue	Description
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.