Release Notes
ArcSight™ Connector Appliance

Version 6.2, Patch 1 (Build C6261.1)

January 17, 2012

ArcSight™
An HP Company

Release Notes ArcSight™ Connector Appliance Version 6.2, Patch 1 (Build C6261.1)

Revision History

Date	Product Version	Description
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

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 Patch 1

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 ArcSight Connector Appliance v6.2 Patch 1 (C6261). Read the entire document before installing this patch.

To maintain optimal operation and performance, ArcSight recommends that all Connector Appliance customers upgrade to this latest patch from 6.2 GA (C6244).

This document discusses the following topics.

What's New in Connector Appliance v6.2 Patch 1

ArcSight Connector Appliance v6.2 Patch 1 resolves known issues for Connector Appliance v6.2 GA.

Users in the Los Angeles Time Zone

If your appliance is set to the Los Angeles time zone, this patch requires that you reset your current time zone to **Tijuana** before applying the patch. After patch installation is complete, you can reset the time zone back to Los Angeles. After any change, reboot the appliance.

Upgrading to v6.2 Patch 1

You can upgrade to Connector Appliance v6.2 Patch 1 from **v6.2 GA (C6244).** 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 v6.2 to v6.2, Patch 1** 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 6.

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 6 for instructions.

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

- `appliance-6261.enc`

  Use this file to perform local upgrades of Connector Appliance v6.2 Patch 1.

- `ArcSight-6.2.0.6261.1-ConnectorAppliance.full.aup`

  Use this file to perform upgrades to remotely managed Connector Appliances.

Preserving Your Remote Management Configuration

ArcSight recommends that you export your remote management configuration before upgrading. To export your 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.

Perform the version 6.2 to 6.2, Patch 1 upgrade. See Upgrading Connector Appliance below for instructions.

Upgrading Connector Appliance

Note

Before you can upgrade remotely-managed appliances, you need to use the `appliance-6261.enc` file to perform local upgrades of Connector Appliance v6.2 Patch 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 6 for instructions.

Upgrading on a Local Connector Appliance

1 Verify that your Connector Appliance is running **v6.2 GA (C6244)**.

To determine the current Connector Appliance version, hover the mouse over the ArcSight logo in the upper left side of the screen. For v6.2, the logo displays `v6.2.0.6244.0`.

You can also click **Setup > System Admin > License & Update** and look for the arcsight-appliance component. For v6.2, the component version is `6.2-C6244`.

2 Download the `appliance-6261.enc` file from the ArcSight software download site at `https://arcsight.subscribenet.com`. Load the file to the computer you use to access the Connector Appliance interface.

3 From the computer to which you downloaded the file, log in to your Connector Appliance.

4 Click **Setup > System Admin** from the top-level menu bar, then click **License & Update** from the **System** section in the left panel.

5 Click **Browse** and select the file.

6 Click U**pload Update**.

Wait until you see a message indicating that the upload was successful.

7 Reboot the appliance.

8 Verify that the Patch is installed:

a Click **Setup > System Admin** from the top-level menu bar, then click **Audit** from the **Logs** section in the left panel.

b In the **Select Date Range** area, select the current date (the date you installed the patch).

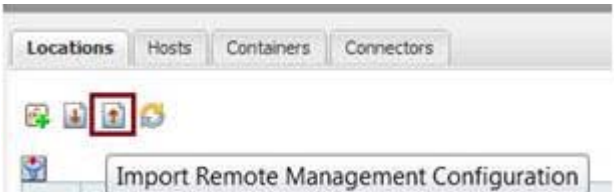
c Click **View Audit Logs**.

d In the Audit Log Search Results table, find **Applied appliance update**.

9 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 at the start of this process under "Upgrading Connector Appliance" on page 7. 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**.

10 See blah to check the configuration.

Upgrading on a Remotely Managed Connector Appliance

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

To determine the version of your remote appliances, click the **Manage** tab. Click **Default** from the left side panel. The main page lists all of the remotely managed host. 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-6.2.0.6261.1-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**.

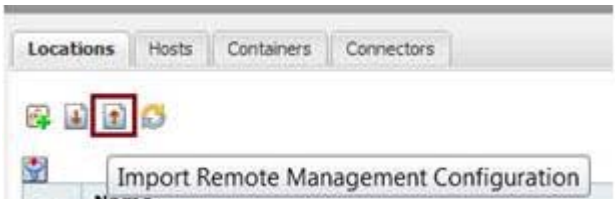
10 From the drop-down list, select `ArcSight-6.2.0.6261.1-ConnectorAppliance.full.aup` and follow the wizard.

When upgrading to any remote Connector Appliance(s), you must login directly to the remotely-managed appliance before performing step 11 below.

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.

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*.

Receiving Events from Microsoft Windows

Connector Appliance can receive events from Microsoft Windows using the Microsoft Windows Event Log Unified SmartConnector. For details on configuring and using this

connector, see the *SmartConnector™ Configuration Guide for Microsoft Windows Event Log—Unified*, available from ArcSight Customer Support.

Remotely Managing Software-Based SmartConnectors

Certain Connector Appliance models can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default. To manage software-based SmartConnectors with the Connector Appliance, you need to enable remote management on the connectors.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies only four SmartConnectors on Windows hosts and eight on Linux or Solaris hosts.

To enable remote management on connectors:

1. Add the following property to the `user/agent/agent.properties` file in the installation directory of each SmartConnector that you want to manage with the Connector Appliance.

   ```
   remote.management.enabled=true
   ```

2. Restart the SmartConnector for the property changes to take effect.

   You can also customize the port on which the connector listens. By default, this port is set to 9001. You can change the port by adding the following property to the `user/agent.properties` file (where *`port_number`* is the port number you want to use; for example 9002).

   ```
   remote.management.listener.port=port_number
   ```

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** > **NFS**) or a CIFS mount (**Setup** > **System Admin** > **Storage**> **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.

In Connector Appliance releases prior to v5.5, certificate validation and host name verification were not supported on the Cisco Secure IDS RDEP and the Cisco Secure IPS SDEE connectors. Connector Appliance v5.5 and later fully supports these connectors; you can use the Certificate Management wizard to add the sensor certificates into the container trust stores before setting up the connectors.

Fixed Issues

The following issues have been resolved in this release.

Issue	Description
CONAPP-3295	When "Internet Explorer 9 standards (Page Default)" was selected in the "Document Mode" menu, the Connector Appliance UI provided a distorted view. Workaround: To prevent this, 1. from the IE 9 browser, choose "F12 developer tools". 2. From the Document Mode drop down menu, choose "Internet Explorer 7 standards".
CONAPP-3290	From the Connector Appliance UI, users were unable to modify and/or delete the Container property from the Manage tab. This issue has been fixed.
CONAPP-3277	If a user selected "Exclude Connector Data" in the backup form, the mechanism would backup AUP files under connectors, creating an excessively large Appliance Backup file. This problem has been fixed, avoiding a large accumulation of files under the /opt/arcsight/connector_x/user/agent/aup folder.
CONAPP-3276	The Russian time zone was displaying incorrectly. This fix allows the Russian time zone to display correctly after their transition away from Daylight Savings Time (DST) in October of 2011.
CONAPP-3228	After an upgrade to v6.2, the Web GUI was slow, most notably on the Manage page. This issue has been fixed.
CONAPP-3209	The logger_web.out.log file failed to rotate, resulting in the file becoming too large and hanging when taking an Appliance snapshot. This issue has been fixed.