Release Notes
ArcSight™ Connector Appliance

Version 6.1 GA (Build C6175)

May 13, 2011

ArcSight™
An HP Company

Release Notes ArcSight™ Connector Appliance, Version 6.1 GA (Build C6175)

Revision History

Date	Product Version	Description
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.
03/10/10	5.5 SP1 Patch 1	Patch 1 for Service Pack 1. Resolved upgrade and memory allocation issues.
01/29/10	5.5 SP1	Removed references to delta upgrade files.
01/25/10	5.5 SP1	Added new feature list, updated upgrade procedure, and added open/closed issues.
09/28/09	5.5 GA	Added new feature list and 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)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal
Protect 724 Community	https://protect724.arcsight.com

Contents

Release Notes
ArcSight Connector Appliance v6.1 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 v6.1 GA (C6175) release. Read the entire document before installing this release.

This document discusses the following topics.

What's New in Connector Appliance v6.1 GA

ArcSight introduces the following new features and enhancements for Connector Appliance v6.1 GA.

- A FlexConnector Development Wizard that lets you quickly and easily develop a FlexConnector. You can create a parser file, and then test and package your new FlexConnector. A FlexConnector Editor Wizard is also provided so that you can edit the FlexConnectors you create.
- Additional Backup and Restore Options. You can now choose what you want to include in your backup file; repository data or connector data, or both.
- Diagnostic Tools on a Container that let you run certain diagnostics on a specific container. This release provides the Edit a File diagnostic tool.
- An updated System Admin menu.
- A new SSH configuration option, which allows the root account to log in to the appliance via SSH to perform administrative tasks, and to troubleshoot and diagnose problems. You can enable SSH access to the appliance permanently, for a period of eight hours, or during appliance startup only. If SSH is enabled and you need to access the appliance with the root account, contact Customer Support to obtain an activation code so that you can log in.

For convenience, you may elect to have SSH always enabled on the appliance so that Customer Support can help you diagnose and resolve Connector Appliance problems at any time.

In order to gain root access to the appliance, you will use an SSH client to connect to the appliance and also call ArcSight Customer Support. Upon connection to the appliance, you will receive a challenge prompt, to which ArcSight Customer Support will provide you with a response. After obtaining an activation code from ArcSight Customer Support, you can log in to the appliance with the root login. When prompted for the password, enter any text and press Enter. You will then be prompted for the activation code.

The session is valid for the amount of time specified in the options described above (any time, a period of eight hours, or at startup only).

Upgrading to v6.1 GA

You can upgrade to Connector Appliance v6.1 GA from Connector Appliance v6.0 Patch2 only.

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 ArcSight Customer Support download site at https://arcsight.subscribenet.com

- `appliance-6175.enc`

  Use this file to upgrade the local Connector Appliance (localhost) to v6.1 GA.

- `ArcSight-6.0.0.6175.0-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 remote Connector Appliances with the `.aup` file from a model C3000 appliance might fail if there is not enough memory for the web process on the C3000 appliance. If your central appliance is a model C3000, upgrade remote Connector Appliances locally with the .enc file.

Upgrading Connector Appliance

You need to upgrade the local appliance (localhost) with the `appliance-6175.enc` file before you can upgrade remotely-managed appliances.

To upgrade Connector Appliance to v6.1 GA

1. Reboot the Connector Appliance.
2. From the ArcSight Customer Support download site (https://arcsight.subscribenet.com), download the `appliance-6175.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. When the upload completes and the reboot message appears, reboot the Connector Appliance.
9. Go to **Setup** > **System Admin > License & Update** and confirm that the Connector Appliance is running v6.1 GA (6.1.0-C6175).

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.

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** > **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.

Closed Issues

The following issues have been resolved in this release.

Issue	Description
CONAPP-2693	The Process Status page displayed incorrect memory usage. This issue has been resolved.
CONAPP-2678	When you made changes to a connector from Connector Appliance, the change was not reflected on the ESM Manager. This issue has been resolved.
CONAPP-2677 TTP#46486	You were unable to upgrade an empty container. This issue has been resolved. You can now upgrade a container that does not contain any connectors to connector version 5.1.2 or later.
CONAPP-2669	Any user logged in to Connector Appliance was able to use the Diagnostic Tools regardless of the user permissions set. This issue has been resolved.
CONAPP-2665	The System Admin menu in the left panel did not display any menu items. This issue has been resolved.
CONAPP-2662	The Content AUP file did not update connectors with new connector event categorization mappings. This issue has been resolved.
CONAPP-2661	Clicking the "Start Reboot Now" button on the Setup > System Admin > Reboot page failed to reboot Connector Appliance.
CONAPP-2648	Appliance backup did not save the contents of the user/agent/checkpoint directory. If you had a Check Point connector and you tried to restore the backup, you lost the certificate files required for communication between the connector and the Check Point server. This issue has been resolved.
CONAPP-2642	Connector Appliance included a vulnerability in the Java Runtime Environment that allowed unauthenticated network attacks. This release includes an update to the Java Runtime Environment (JRE) on Connector Appliance to address the Security Alert for CVE-2010-4476.
CONAPP-2621	See CONAPP-2585.
CONAPP-2612	The Diagnostic Tools page and the Support Login page did not display. The Diagnostic Tools page now displays in the right panel. The Support Login page has been replaced with the SSH page.
CONAPP-2592	If you tried to add an ESM destination without first applying a certificate on the container, you saw the error message "Following error occurred [null]."
CONAPP-2585	When you rebooted Connector Appliance, the connector processes failed to stop, which prevented the appliance from rebooting and left the appliance in a degraded state. You also saw that Process Status page was empty. The appliance remained in a reboot pending state and did not reboot successfully until after the connector processes stopped.
CONAPP-2568	The URL for Connector Appliance specified logger instead of conapp. After upgrading to Connector Appliance v6.1, make sure you delete your browser history.
CONAPP-2533	When using the "Ping host" diagnostic tool, you were unable to enter more than 15 characters in the Host field. The maximum number of characters allowed in the Host field has been increased to 255.
CONAPP-2525	If Connector Appliance contained 11 or more Windows hosts and you tried to add or remove additional hosts, you saw the error message "No Parameters were updated."

Issue	Description
CONAPP-2449	The EPS Out and EPS In columns in the table on the Connectors tab displayed a long value. The EPS Out and EPS In values are now limited to a maximum of two decimal places.
CONAPP-2434	When creating an SSL certificate, the CSR failed to generate if the private key included special characters.
CONAPP-2415	When you upgraded a container from 5.0.2 to 5.0.3 or later, the container status on the Setup > System Admin > Process Status page showed that the container did not exist even though the container was running and sending events.
CONAPP-2414	If the State/Province or City/Locality field on the Generate Certificate Signing Request page included a space, Connector Appliance displayed the error message "State is invalid" or "Locality is invalid" when trying to generate the CSR. This issue has been resolved.
CONAPP-2406	When you exported connector parameters that contained encrypted fields to a file and then imported the file to another connector in a different container, an error message displayed or the container became unavailable. ArcSight recommends that you do not export connector parameters from one connector and import them to another connector on a different container.
CONAPP-2376	The Diagnostic Tools, Support Login, SSL Client Authentication, and FIPS 140-2 pages did not always display. This issue has been resolved.
CONAPP-2363	When you upgraded a remotely-managed Connector Appliance with the AUP upgrade file, a message displayed indicating that the upgrade failed. This issue has been resolved.
CONAPP-2340	The Send Command wizard displayed an error message with the word command spelled incorrectly. This spelling mistake has been corrected.
CONAPP-2266	The value for DeviceProduct in system health events was inconsistent, which made tracking events in reports and alerts difficult. This issue has been resolved.
CONAPP-2076 TTP#68965	When importing a remote management configuration, Connector Appliance scanned all ports when searching for remote hosts instead of only the ports specified in the software manager configuration. This issue has been resolved; Now, only the ports specified are scanned.
CONAPP-1782 TTP#65412	The login banner did not display after a successful CAC login. This issue has been resolved.
CONAPP-1766 TTP#65193	The Update Connector Parameters wizard did not include the Export to File button that enables you to export parameters to a CSV file. The Export to File button is now included.
CONAPP-1732 TTP#64388	You were unable to back up Connector Appliance to your local computer. This option has been added to the Protocol field on the Appliance Backups tab (Setup > Backup/Restore > Appliance Backup).
CONAPP-1662 TTP#62910	Connector Appliance did not have an option for specifying the length of the private key when generating a Certificate Signing Request (CSR). The "Private Key Length" field has been added to the Generate CSR tab (Setup > System Admin > SSL Server Certificate).
CONAPP-1509 TTP#60182	When you added a CIFS mount, log file connectors, such as the Symantec AntiVirus connector, did not receive new events even though the events were listed in the log file.
CONAPP-1398 TTP#59215	If you imported a CSV file of hosts for Windows Unified connectors and specified the value "TRUE" in upper case, the value was not imported correctly. This issue has been resolved; the value "true" is now case-insensitive.

Issue	Description
CONAPP-1263 TTP#58056	When restoring Connector Appliance from a backup file that is larger than 200 MB, the error message "The file specified is too large (200MB maximum)" displayed. You can now restore a backup file that is larger than 200 MB.
CONAPP-1220 TTP#57533	The table parameters wizard for the Windows Unified connector did not include the Export File button. In addition, after importing a CSV file, the Event Log types were not updated correctly for Security, System, and Application events. These issues have been resolved.

Open Issues

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

Issue	Description
CONAPP-2810	Upgrading remote Connector Appliances with the .aup file from a model C3000 appliance might fail if there is not enough memory for the web process on the C3000 appliance. Workaround: Upgrade the remote Connector Appliances locally with the .enc file.
CONAPP-2734	If you reboot the appliance, log back in to Connector Appliance and then click the Setup > System Admin menu, the ArcSight Logger Login page sometimes displays. Workaround: Wait approximately three minutes after the system reboots before logging back in to Connector Appliance.
CONAPP-2724	You are unable to delete a user that is currently logged in or has logged out recently. Workaround: After the user has logged out, wait a few minutes before deleting their account. Alternatively, you can mark the user account inactive; Go to Setup > System Admin > Users/Groups > User Management. On the Users tab, select the user and click the Edit button. On the Edit User page, uncheck the Active box, then click Save and Close.
CONAPP-2655	After you back up and restore Connector Appliance, the CIFS mount is not available. Workaround: Edit the CIFS mount (Setup > System Admin > CIFS), and 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, you see a warning message indicating that the connection to the destination failed on a ping test even if all the destination parameters are correct and the SSL certificate for the Logger appliance is imported correctly into the connector trust store.
CONAPP-1999 TTP#68340	RAID and Sensor internal events are not generated.