Release Notes
ArcSight™ Connector Appliance

Version 6.0 GA (Build C6017)

September 20, 2010

Release Notes ArcSight™ Connector Appliance, Version 6.0 GA (Build C6017)

Revision History

Date	Product Version	Description
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.
08/26/09	5.1 Patch 1	Added closed issues.
07/15/09	5.1 GA	Added new feature list, upgrade instructions, known behaviors, and open/closed issues.
01/13/09	5.0 Patch 2	Updated for Patch 2.
10/14/08	5.0 Patch 1	Added open/closed issues post-v5.0 release.
09/17/08	5.0	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 v6.0 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 v6.0 GA (C6017) release. Read the entire document before installing this release.

This document discusses the following topics.

What's New in Connector Appliance v6.0 GA

ArcSight introduces the following new features and enhancements for Connector Appliance v6.0 GA.

- Diagnostic Tools

  You can run commands directly from the Connector Appliance UI to help diagnose network and application issues. These diagnostic tools are provided in the **Setup** > **System Admin** > **Diagnostic Tools** menu:

  - **Display file** displays the contents of a file.
  - **Display network connections** shows network connections and transport protocol statistics.
  - **Display network interface details** shows the status of a currently active interface on the appliance.
  - **Display network traffic** monitors packets that are transmitted and received on the network.
  - **Display process summary** lists the currently running processes and shows how long they have been running.
  - **Display routing table** shows the routes through which traffic flows from the appliance.
  - **Edit text file** lets you edit files on the appliance.
  - **List directory** displays the contents of a directory on the appliance.
  - **List processes** displays the top CPU processes that are currently running together with memory and resource information.
  - **Ping host** lets you test if a particular host is reachable across an IP network and measure the round-trip time for packets sent from the appliance to the host.
  - **Resolve hostname** looks up a hostname in the Domain Name Server and converts it to an IP address.
  - **Scan network ports** scans a specific host on the network for open ports.
  - **Send signal to container** sends a terminate command to a container.
  - **Tail file** displays the last ten lines of a system, application, or log file.
  - **Trace network route** displays the specific network route between the appliance and a specified host.

- ArcExchange Integration (sharing FlexConnectors and parser overrides)

  You can upload and download FlexConnectors and parser overrides to and from the ArcSight Community web site (Protect 724) or your local computer. To upload FlexConnectors and parser overrides, the  icon is available at the top of the **Manage** > **Connector** page and on the **Action** column of the **Manage** > **Connectors** page. To download FlexConnectors and parser overrides, the icon is available on the **Action** column of the **Manage** > **Containers** page.

- Remote Management Configuration

  You can now export the remote management configuration of your Connector Appliance and import it on another appliance. The **Manage** > **Locations** page includes two new icons:  enables you to export the remote management configuration of your Connector Appliance and  enables you to import the remote management configuration of a different Connector Appliance.

  

  The containers running locally are not included in the remote management configuration.

- Destination Enhancements

  The **Destinations** button on the **Manage** > **Connectors** page provides new options to perform destination tasks on several SmartConnectors at the same time. In previous releases, the **Destinations** button was called **Add Destinations**.

- Connector Parameter Editor Enhancements

  The new **Parameters** button on the **Manage** > **Connectors** page provides options to edit both simple and table parameters on multiple SmartConnectors at the same time.

- Appliance Backup and Restore Enhancement

  During appliance backup (**Setup** > **Backup/Restore** > **Appliance Backup**), you can choose between creating a backup file that contains all data and configuration settings on the appliance or a backup file that excludes SmartConnector data stored in the cache.

Upgrading to v6.0 GA

You can upgrade to Connector Appliance v6.0 GA from **v5.5 SP1 Patch 1 (C5581)** 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-6017.enc`

  Use this file to upgrade the local Connector Appliance (localhost) to v6.0 GA.

- `ArcSight-6.0.0.6017.0-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-6017.enc` file before you can upgrade remotely-managed appliances.

To upgrade Connector Appliance to v6.0 GA

1. Reboot the Connector Appliance.
2. From the ArcSight Customer Support download site (https://arcsight.subscribenet.com), download the `appliance-6017.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. Click **License & Update** under **System** in the left panel.
6. Click **Browse** to locate the upgrade file you downloaded in Step 2.
7. Click **Upload Update**.
8. Wait for the upload to complete and the reboot message to appear, and then reboot the Connector Appliance.
9. Go to **Setup** > **System Admin > License & Update** and confirm that the Connector Appliance is running v6.0 GA (6.0.0-C6017).

Information You Need to Know

This section highlights important Connector Appliance information.

Hardware Installation

The sliding rails shipped with the C3200 and C5200 appliances are designed for use with the 4-post equipment racks only. ArcSight recommends that you do not use the 2-post rack for the C3200 and C5200 appliances.

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*.

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.

Closed Issues

The following issues have been resolved in Connector Appliance v6.0 GA.

Number	Description
TTP#52603 CONAPP-900 TTP#69684 CONAPP-2253	In Windows Internet Explorer, you were unable to paste a large number of entries in the system hosts file (Setup > System Admin > Network > Hosts tab).
TTP#52695 CONAPP-902	The Connector Appliance login page was vulnerable to cross-site scripting attacks. This is no longer an issue.
TTP#59583 CONAPP-1452	The Connectors tab displayed `UNKNOWN` in the EPS In and EPS Out columns even though data was being transferred.
TTP#59636 CONAPP-1458	The logs for a connector configured with a CIFS mount point displayed the error message `Output in unexpected format`.
TTP#60998 CONAPP-1545	After you backed up and restored the Connector Appliance (Setup > Backup/Restore), the connectors failed to register with ESM because the certificates were not applied to the container.
TTP#61573 CONAPP-1567	When backing up the Connector Appliance configuration, the backup process timed out and then failed. This issue has been resolved.
TTP#62064 CONAPP-1598	You were unable to restore a backup Connector Appliance configuration file that was 200 MB or larger.
TTP#62089 CONNAPP-1601	When you rebooted a Connector Appliance with a CIFS mount point, the appliance became unresponsive.
TTP#62836 CONAPP-1655	When FIPS mode was enabled on a container and an ArcSight Logger was set as a forwarding destination, events were not forwarded if the Logger was using the default demo certificate. Refer to the article "FIPS-enabled connector will cache to any Logger destination using demo/default certificate" in 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.
TTP#67489 CONAPP-1924 TTP#69179 CONAPP-2101	If you restarted a container from the Setup > System Admin > Process Status page, the container status sometimes showed the message `Execution failed` or `Does not exist` even though the container was running. This issue has been resolved for connectors running build 5.0.2.5670 or later. **Note**: Reboot the appliance to update the container status.
TTP#66859 CONAPP-1858 TTP#69112 CONAPP-2093	Microsoft SQL Server connectors with a CIFS mount point caused Connector Appliance to freeze if the CIFS mount point did not have write permissions.

Number	Description
TTP#66869 CONAPP-1859 TTP#67458 CONAPP-1917 TTP#68769 CONAPP-2045 TTP#68865 CONAPP-2057	All known connector upgrade issues on Connector Appliance have been resolved.
TTP#69295 CONAPP-2110	The Connector Appliance `catalina.out` log files did not rotate and filled up disk space. The log files now rotate correctly and there are no disk space issues.
TTP#69335 CONAPP-2115	When a connector was configured with a CIFS mount point and the CIFS mount point became unreachable, the connector became unresponsive. **Note**: This issue has been resolved for Connectors running version 5.0.2.5642 and later.
TTP#69354 CONAPP-2118 TTP#69403 CONAPP-2240	The CPU gauge on the Monitor page displayed incorrect CPU utilization data.
TTP#69412 CONAPP-2124	When you added the Symantec EndPoint Protection Database connector to a container on Connector Appliance, you sometimes saw the error message `Database version could not be detected`. This error occurs if an event type is entered during connector configuration for which no data exists. Refer to the *Symantec EndPoint Protection DB Connector Configuration Guide* for more details.
TTP#69428 CONAPP-2126	When you removed the middle table entry for database connectors on Connector Appliance, the secret parameter in the next table entry was not set correctly. As a result, events were not received.
TTP#69745 CONAPP-2239	After restoring a container (Setup > Repositories > Emergency Restore), the container failed to start.
CONAPP-2296	When you upgraded Connector Appliance to v5.5 SP1 or v5.5 SP1 Patch 1, permissions were not upgraded correctly. This issue has been resolved. When you upgrade to Connector Appliance v6.0, permissions are upgraded correctly.

Open Issues

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

Number	Description
TTP#43480 CONAPP-194	URLs for the Connector Appliance show Logger.
TTP#43643 CONAPP-217	When a configuration backup fails during restore, the wrong window displays, resulting in nested frames. **Workaround**: Restart the browser and log in again.
TTP#49855 CONAPP-3121	When you make changes to default settings on ArcSight ESM, the destination-specific configuration settings on Connector Appliance are overwritten.
TTP#52040 CONAPP-889	If you navigate to another page while creating a new connector, the parameters already entered for the new connector are lost.
TTP#60677 CONAPP-1538 TTP#62846 CONAPP-1656	Containers display in the FIPS Status table under Setup > System Admin > Security > FIPS 140-2 and can be FIPS enabled only when all the containers are version 4.7.5 or later, and are reachable. **Workaround**: Before enabling FIPS mode, be sure to upgrade all containers to version 4.7.5 or later.
TTP#62415 CONAPP-1628 TTP#69113 CONAPP-2094	Due to an unknown JVM issue, containers constantly restart and their status shows `unknown` or `down`. **Workaround**: Reboot the Connector Appliance.
TTP#65399 CONAPP-1780	If you enable FIPS mode immediately after upgrading a container, the container displays the previous version number, FIPS mode is disabled, and the container becomes unavailable. **Workaround**: After upgrading a container, wait approximately 10 minutes before enabling FIPS mode.