Release Notes
ArcSight™ Connector Appliance

Version 6.0 Patch 2 (Build C6023)

November 22, 2010

Release Notes ArcSight™ Connector Appliance, Version 6.0 Patch 2 (Build C6023)

Revision History

Date	Product Version	Description
11/22/10	6.0 Patch 2	Added resolved issues.
10/18/10	6.0 Patch 1	Added resolved update issue.
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.

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 Patch 2

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 v6.0 Patch 2 (C6023). ArcSight recommends that you read the entire document before installing this patch.

This document discusses the following topics.

What's New in Connector Appliance v6.0 Patch 2

ArcSight Connector Appliance v6.0 Patch 2 resolves known issues. For a list of the resolved issues, see "Fixed Issues" on page 7.

Upgrading to v6.0 Patch 2

You can upgrade to Connector Appliance v6.0 Patch 2 from the following versions.

- **v6.0 Patch 1 (C6020)**
- **v6.0 GA (C6017)**

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-6023.enc`

  Use this file to upgrade the local Connector Appliance (localhost) to v6.0 Patch 2.

- `ArcSight-6.0.0.6023.2-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-6023.enc` file before you can upgrade remotely-managed appliances.

To upgrade Connector Appliance to v6.0 Patch 2

1. Reboot the Connector Appliance.
2. From the ArcSight Customer Support download site (https://arcsight.subscribenet.com), download the `appliance-6023.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 Patch 2 (C6023).

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.

Fixed Issues

The following issues have been resolved in this patch.

Issue	Description
CONAPP-2402	If you uploaded a file to a repository and then clicked on another repository straight away, an exception displayed on the user interface without any explanation. A message is now provided with an explanation of the problem.
CONAPP-2385	When editing the Domain User Password parameter on the Windows Unified Connector, the password was not encrypted correctly if you used special characters. This issue has been resolved and the password is now encrypted correctly.
CONAPP-2383	In the Add Destination wizard, after choosing "Select an existing destination," the connector name displayed at the beginning of each selection. The list has been modified to display the destination type at the beginning of each selection.
CONAPP-2381	If the Domain Password on a connector was set in the agent.properties file, the Domain Password field was empty under the connector parameters on Connector Appliance and you were unable to delete the password. The Domain Password field now displays the characters as dots and you are able to delete the password.
CONAPP-2380	When changing a password for the Windows Unified connector or a Database connector, you saw an error message similar to the following: "Connector table parameters did not pass verification with error [0:Could not connect to host [10.10.10.10]]. Do you still want to continue?" This issue has been resolved and the error message no longer displays.
CONAPP-1858 TTP#66859	Microsoft SQL Server connectors with a CIFS mount point caused Connector Appliance to freeze if the CIFS mount point did not have write permissions. You now see a message on the user interface asking you to check permissions before mounting the CIFS share.

Open Issues

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

Issue	Description
CONAPP-2415	When you upgrade a container from 5.0.2 to 5.0.3 or later, the container status on the Setup > System Admin > Process Status page shows that the container does not exist even though the container is running and sending events. Workaround: Go to Setup > System Admin > Reboot and reboot Connector Appliance.
CONAPP-2406	When you export connector parameters that contain encrypted fields to a file and then import the file to another connector in a different container, an error message displays or the container becomes 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 sometimes do not display. ArcSight is currently investigating this issue.
CONAPP-2363	When you upgrade a remotely-managed Connector Appliance with the AUP upgrade file, a message displays indicating that the upgrade failed. Workaround: You can safely ignore this message; the upgrade completes successfully.
CONAPP-2358 TTP#49855	When you make changes to default settings on ArcSight ESM, the destination-specific configuration settings on Connector Appliance are overwritten.
CONAPP-1780 TTP#65399	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.
CONAPP-1656 TTP#62846	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.
CONAPP-1628 TTP#62415	Due to an unknown JVM issue, containers constantly restart and their status shows unknown or down. Workaround: Reboot the Connector Appliance.
CONAPP-1538 TTP#60677	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.
CONAPP-889 TTP#52040	If you navigate to another page while creating a new connector, the parameters already entered for the new connector are lost.
CONAPP-217 TTP#43643	When a configuration backup fails during restore, the wrong window displays, resulting in nested frames. Workaround: Restart the browser and log in again.
CONAPP-194 TTP#43480	URLs for the Connector Appliance show Logger.