Release Notes for Cisco VSM 7.2 Driver Pack, Release 2.0-32

October 18, 2013

This document provides important information for the Cisco Video Surveillance Manager (VSM) 7.2 driver pack release 2.0-32.

This document includes the following sections:

What's New in this Release

This release provides the ability to receive analytics events from Cisco 4xxE camera models that are running firmware version 3.2.3-218 or higher and from Cisco 4xxx camera models that are running firmware version 2.4.2-289 or higher.

Important Notes

- Medianet support:
  - VSM 7.2 supports new Medianet features including Metadata, Performance Monitoring, and Mediatrace. These features are supported on the Cisco 2830, 2835, 3421, 3520, 3530, 6000 series, 6930, and 7030 cameras. The minimum supported firmware version for this feature is 1.4.1. See the "Medianet 2.0 Support" section in *Release Notes for Cisco Video Surveillance Manager Release 7.2.0* for more information. Cameras with the earlier firmware versions support only the Medianet 1.0 features from Cisco VSM Release 7.0.1.
  - The Cisco 2600 series, 4300, 4300E, 4500, and 4500E cameras support only the Medianet 1.0 features in VSM 7.0 and 7.0.1.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Cisco 4500 and 4500E cameras support video analytics.
- Redundancy is supported for all Cisco cameras, with some exceptions for the 2400, 2500, 2900, and 5000 series. The 2400, 2500, 2900, and 5000 series do not support sending events such as motion detection and contact closure to the redundant server.
- The Cisco 5000 series cameras do not support motion detection at video bit-rates above 4,000 (4 Mbps). The "H" video preset in the templates has been chosen to not exceed this value, so motion detection will work.
- The Cisco 5000 and 2900 series cameras do not allow changes to the authentication settings (username/password) or networking settings (including DHCP/Static, DNS) through VSM. These values can be changed by using the camera web interfaces.
- Support for the focus, auto focus, and zoom camera controls are not available on Cisco 6000P, 3421V, 3520, and 3530 camera models.
- When VSM manages a Cisco 6930, 2830, or 2835 camera, it automatically enables the HTTP protocol on the camera and uses this protocol to send PTZ commands to the camera. Other configuration commands continue to use the HTTPS protocol.
- The Cisco 2830, 2835, 3000 series, 6000 series, and 7030 cameras now support MJPEG primary streams. The minimum supported firmware version for this feature is 1.4.1.
- Resolution support:
  - Support for 352 x 208, 704 x 400, and 768 x 432 resolutions for both primary and secondary streams on Cisco 3000 series, 6000 series, and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
  - The following additional resolutions are available for the 6930 cameras: 1536 x 864, 1472 x 832, 768 x 432, 704 x 400, 352 x 208, 320 x 192, 192 x 112, and 160 x 96. The minimum supported firmware version for this feature is 1.4.1, and VSM 7.2 is required.
  - Support for 1536x864, 1472x832, 720x576, 704x576, 352x288 for the Cisco 6000 series and 7030 models, support for 2560x1920 resolutions for the Cisco 7030.
  - Support for 1Mbps bitrate for the 1920 x1080 resolution on Cisco 6000 series and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
  - Support for 1.5 Mbps bitrate for certain resolutions on Cisco 2830, 2835, 3000 Series, 6000 series, and 7030 cameras. The minimum supported firmware version for this feature is 1.3.2-8.
- Contact closure:
  - Cisco 3000, 6000 series cameras support one input port.
  - Cisco 7030 camera supports three input ports
  - Cisco 6930, 2830 and 2835 cameras support all four contact closures
  - Cisco 3421V cameras do not support contact closure

In PTZ Tour Configuration, the configured transition time includes the time that it takes the camera to move from one preset position to the next preset position in addition to the time that the camera is expected to stay in the preset position. If the transition time is configured to a value that is less than the time that it takes the camera to move from one preset position to the next, the camera moves between the first and second presets positions only, instead of touring between all preset positions that are configured in the tour.

Supported Devices

Table 1 lists the Cisco devices that this driver pack supports.

Table 1 Cisco Devices that this Driver Pack Supports

Cisco Model	Recommended Minimum Firmware Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Medianet
2400 Series	2.5.0-9	NTSC PAL	MPEG-4 MJPEG	No	Yes	Yes	Yes	No
2500 Series	2.5.0-9	NTSC PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
2600 Series	4.4.0-13	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes
2830	1.2.2-20	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
2835	1.2.2-20	PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
3421V	1.3.2-8	NTSC PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes
3520	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
3530	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4300	2.4.2-289	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4300E	3.2.3-218	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4500	2.4.2-289	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
4500E	3.2.3-218	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
6000P	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
6020	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
6030	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
6400	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
6930	1.2.2-20	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes

Table 1 Cisco Devices that this Driver Pack Supports (continued)

Cisco Model	Recommended Minimum Firmware Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Medianet
7030	1.3.2-8	NTSC PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes
CIVS-SENC-4P	1.1.0-1	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
CIVS-SENC-8P	1.1.0-1	NTSC PAL	H.264 MPEG-4 MJPEG	Yes	—	Yes	Yes	No

Obtaining and Installing the Driver Pack

You obtain by using a client PC from which you can access the Cisco.com website.

Driver packs must be upgraded to the same version on each server on which the Media Server and Operations Manager services are enabled. For example, if your deployment includes a standalone Operations Manager, the Operations Manager server must have the same driver pack versions as the Media Servers that are associated with that Operations Manager. If the versions are different, a driver pack mismatch error can occur, which prevents camera template revisions.

To obtain and install the driver pack, follow these steps. The driver pack must first be installed on the VSOM server and then on each VSMS server.

Procedure

Step 1 From a client PC that can access Cisco.com, take these actions to obtain the driver pack:

a. Go to this URL (you must have a valid Cisco.com user ID and password before you can access this URL):

http://software.cisco.com/download/release.html?mdfid=282976740&softwareid=282074157&release=7.2.0&relind=AVAILABLE&rellifecycle= &reltype=latest

b. Click the **Video Surveillance Device Driver** link.

c. Click **Latest Releases > 7.0.0** in the panel on the left of the window.

d. Click the **Download** button for the **dp_cisco-2.0-32d_7.2.0-020d.zip** driver pack.

e. Follow the on-screen instructions to download the driver pack file.

Step 2 From a client PC that is running Microsoft Windows 7 and that can access the VSM Management Console, start a 32-bit version of Internet Explorer.

Step 3 In the Internet Explorer Address field, enter the following URL, replacing *server* with the IP address or host name of the VSOM server in your deployment:

https://*server*

Step 4 Log in to the VSM Management Console and take these action to install the driver pack:

a. Choose **System Settings > Driver Pack Management**.

b. (Optional) Choose the filters to display specific servers. (All servers are displayed if no filters are selected.)

c. Click **Search** to display the list of servers according to the filters.

d. Choose a server to display the driver packs that are installed on that server.

e. Upload the new driver pack software file to the Operations Manager server:

   1. Click the **Manage** tab.
   2. Click **Add**.
   3. In the pop-up window choose **dp_cisco-2.0-32d_7.2.0-020d** from a local or network disk.
   4. Click OK and wait for the drivers to upload to the Operations Manager server. The driver pack status is "Not Installed".

f. Copy the new driver pack from the Operations Manager server to the other servers.

   (Copying the driver pack to the other servers allows the Media Servers to be upgraded.)

   1. Click the **Driver Pack Upgrade** tab.
   2. Choose one or more servers.
   3. Click **Copy To Server**.
   4. Click the **Manage** tab

      (You can copy the driver pack to the servers without installing it, which allows you to stage the software on a server without performing the upgrade, if necessary.)

g. Install the new driver pack on the servers:

   1. Choose one or more servers from the **Driver Pack Upgrade** tab.
   2. Click **Install** to install all driver packs that were copied to the server.

Driver packs can only be upgraded. They cannot be downgraded.

Caution Caution Do not refresh the browser while the driver installation is in progress.

Caveats

The following sections provide information about caveats in this Cisco IPICS release:

Using the Bug Search Tool

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

Note Bug Search Tool is the successor to the Bug Toolkit.

To use the Bug Search Tool, follow these steps:

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the Search For field, then press **Enter**.

Step 4 To look for information if you do not know the bug ID number, enter keywords which search for text matches in the following sections of a bug:

- headline/title
- release note text
- product
- known affected releases/ known fixed releases

For more information about the Bug Search Tool, click Help on the main Bug Search Tool page:

https://tools.cisco.com/bugsearch/

Resolved Caveats

Table 2 describes resolved caveats in this release.

Table 2 Resolved Caveats

Headline	Description
CSCuj12461	VSM does not receive analytic events from new 4xxxE/4xxx firmware