Release Notes for Cisco Video Surveillance Manager, Release 7.14.7

Revised: July 7, 2023

Note **Always refer to the latest online version of these Release Notes for up to date information.**

This document provides important information for Release 7.14.7 of the Cisco Video Surveillance Manager (Cisco VSM).

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Cisco VSM Release 7.14.7 includes bug declarations.

- Direct upgrade of any VSM version prior to 7.14.5 to 7.14.7 is *not* recommended or tested. Upgrade to 7.14.5/7.14.6 from previous versions and then upgrade to VSM 7.14.7.
- Upgrade to 7.14.7 is *not* supported on the Cisco CSS UCS series servers CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9.
- Upgrade to 7.14.7 is *not* supported for servers deployed on ESXi5.1.
- 7.14.7 has been tested on Internet Explorer 10 and higher, Chrome, Firefox browsers *only*.

Support for RHEL 8.4

VSM release 7.14.7 runs on RHEL 8.4. Upgrades to release 7.14.7 will first upgrade the RHEL operating system and then the Cisco VSM system software. Status is displayed on the UI during the RHEL upgrade.

Getting Started

Cisco VSM Release 7.14.7 is pre-installed on new servers, can be installed as a virtual machine, or used to upgrade an existing deployment.

Table 1 Cisco VSM Installation and Upgrade Options

Option	Description	Notes
Pre-installed	Release 7.14.7 is pre-installed in new installations on the Cisco Connected Safety and Security UCS Platform Series servers: • KIN-UCSM5-1RU-K9 / KIN-UCSM5-2RU-K9	See Cisco Connected Safety and Security UCS Platform Series Servers, page 3 for more information.
Upgrade from a previous release	Direct upgrades can be performed from the previous 2 releases. i.e., 7.14.5 and 7.14.6. Upgrades can be performed on Cisco VSM virtual machines (VMs) and on Cisco Video Surveillance servers.	See Upgrading from Previous Cisco VSM Releases.
Virtual Machine (OVA templates)	An .OVA template file is used to install a new virtual machine (VM) instance of the server.	After an .OVA virtual machine is installed, you can use the Cisco VSM Management Console to perform future upgrades of the system software. See Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

See the following for more information:

- Cisco Video Surveillance Manager: Install and Upgrade Guide
- Cisco Connected Safety and Security UCS Platform Series Servers, page 3
- Upgrading from Previous Cisco VSM Releases, page 3
- Recovery/Factory Image, page 5

Cisco Connected Safety and Security UCS Platform Series Servers

Cisco VSM Release 7.14.7 is pre-installed on new installations of the Cisco Connected Safety and Security UCS Platform Series when ordered with the Cisco VSM software installed.

Supported Servers

- KIN-UCSM5-1RU-K9 / KIN-UCSM5-2RU-K9

Related Documentation

- Cisco CSS UCS Server User Guide— supported features, physical installation and setup instructions
- Release Notes for the Cisco CSS UCS Servers

Notes

- After the server appliance is installed, see the Cisco Video Surveillance Manager: Install and Upgrade Guide to perform the initial Cisco VSM setup.
- For additional server hardware documentation, see the Cisco UCS C-Series Server Documentation (Roadmap).

Upgrading from Previous Cisco VSM Releases

For complete instructions, see the Cisco Video Surveillance Manager: Install and Upgrade Guide.

Important notes before you upgrade:

1. Direct upgrade of any VSM version prior to 7.14.5 to 7.14.7 is *not* recommended or tested. Any server/setup prior to version 7.14.5 must be upgraded to 7.14.5 or 7.14.6 and then upgraded to VSM 7.14.7.

Follow rest of the instructions to upgrade VSOM and servers mentioned in Table 2, Row 1.

2. VSM with SAN storage has issues. Please see Appendix below before upgrade/install 7.14.7
3. External storage SAN has not been tested with VSM-7.14.7. Media partitioning using NAS and LVM has not been tested.
4. SASD upgrade may fail in the following scenarios while upgrading VSM from 7.14.x to 7.14.7.

   4.1. Auto-upgrade Video Wall - In this scenario, the SASD video wall upgrade fails and the download process get stuck indefinitely.

   4.2. Downloading SASD after connecting to VSOM - In this scenario, when the user clicks on the 'download' option after connecting to the upgraded VSOM from SASD, the download process gets stuck forever.

   WORKAROUND
   Install SASD by following the download and install instructions present in the user guide under section “Installing the Application Suite.”

5. We recommend taking a snapshot of all your VMs using ESXi or VCenter. Take the latest backup of all your servers using CDAF before you upgrade.

Upgrade methods

The following table describes the upgrade methods based on how old your server's current release is.

Table 2 Upgrade Methods

Upgrading From...	Upgrade Method	More Information
Upgrade from version 7.14.5/7.14.6 to 7.14.7	For direct upgrade from 7.14.5/7.14.6 to 7.14.7 using .zip upgrade, please follow the steps mentioned in next column. (Prerequisite: VSOM/ VSF needs to be upgraded first)	For VSOM and associated servers. • Upgrade VSOM/VSF server: Login to CDAF UI of VSOM/VSF server and upload .zip upgrade file and install. • Upgrade associated Media servers: Login to VSOM and upload .zip file. Copy to servers and install .Cisco Video Surveillance Manager: Install and Upgrade Guide
Direct upgrade from any VSM version prior to 7.14.5 to 7.14.7 is not recommended or tested. Upgrade from previous versions and then upgrade to 7.14.7 as described above.		
Release 7.6 and later (except for 2 most recent releases)	Backup and restore to a new server For example, backup the configuration and data from a release 7.9 server and restore it to a new release 7.14 server. **NOTE** - Only backups that include configuration+ historical data are supported for upgrades. Configuration-only backups are not supported and will cause a config mismatch in the cameras	Cisco Video Surveillance Manager: Install and Upgrade Guide (see "Upgrade Procedure Summary") This method was introduced in release 7.10.
Release 7.2 and earlier	For older releases, first upgrade to 7.6 then upgrade to latest version.	See the following for your release: • Cisco Video Surveillance Manager: Install and Upgrade Guide • Cisco Video Surveillance Management Console Administration Guide • Release Notes for Cisco Video Surveillance Manager

Platform Notes

- **Release 7.0** was pre-installed on the Cisco Multiservices Platform (Cisco MSP) servers, including the CPS-MSP-1RU-K9 and CPS-MSP-2RU-K9.
- **Release 7.2 to Release 7.7** was pre-installed on the CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9 Cisco CSS UCS series servers.

  - The CIVS platform is not supported and cannot be upgraded to VSM 7.7 or later.
- **Release 7.7 to 7.11.1** is also pre-installed on the Cisco CSS UCS series servers:
  - CPS-UCSM4-1RU-K9 / Cisco CPS UCSM4 2RU
- **Release 7.11.1 and higher** is also pre-installed on the Cisco CSS UCS series servers:
  - KIN-UCSM5-1RU-K9 / KIN-UCSM5-2RU-K9
- **Release 7.14.7 is not supported on the Cisco CSS UCS series servers**
  - **CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9**
- **Release 7.14.7 is not supported on ESXi 6.5 and earlier**

Note Virtual Machine (VM) installations can also be upgraded using the Cisco VSM Management Console. Upgrades are supported from release 7.11 or higher on the RHEL 6.10 and 7 operating systems. See Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Recovery/Factory Image

You can also create a bootable USB flash drive that can be used to recover an installation or perform a a factory installation of Cisco VSM Release 7.14.7 on a supported physical server that shipped with Cisco VSM Release 7.14.7 pre-installed. This includes KIN-UCSM5-1RU-K9 and KIN-UCSM5-2RU-K9.

For more information, see Cisco Video Surveillance Manager: Install and Upgrade Guide

Released Versions

Cisco VSM Release 7.14.7 is released with Cisco_VSM-7.14.7-24i The component package versions are:

- Cisco_VSMUpgrade-7.14.7-060d.x86_64
- Cisco_VSMS-7.14.7-060d.x86_64
- Cisco_GeoServer-7.14.7-4.noarch
- Cisco_MetaDataService-7.14.7-060d.x86_64
- Cisco_AMQBroker-7.14.7-1.noarch
- Cisco_VSDrivers-7.14.7-060d.x86_64
- Cisco_Tomcat-7.0.109-1.el7.noarch
- Cisco_CDAF-7.14.7-23.noarch
- Cisco_MPClient-7.14.7-26.noarch
- Cisco_VSRecorder-7.14.7-060d.x86_64
- Cisco_VSBase-7.14.7-060d.x86_64
- Cisco_VSF-7.14.7-23.noarch
- Cisco_DashCast-7.14.7-060d.x86_64
- Cisco_VSTools-7.14.7-060d.x86_64

- CCisco_VSOM-7.14.7-23.x86_64
- Cisco_SASD-7.14.7-2.noarch

Supported Devices

The following sections provide information about the devices that this version of Cisco VSM supports:

Supported Devices: Cisco

Table 3 through Table 9 provide information about Cisco devices supported in this release:

- Cisco 2400/2500, 2600, 2800, and 2900 Series
- Cisco 3000 Series
- Cisco 4000 Series and 5000 Series
- Cisco 6000 Series
- Cisco 7000 Series
- Cisco 8000 Series
- Cisco CIVS-SENC-4P and CIVS-SENC-8P

Table 3 Cisco 2400/2500, 2600, 2800, and 2900 Series

Basic functionality such as streaming and recording are supported. Any features that require a firmware upgrade are not supported.

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
2400 Series	Minimum: 2.5.2.2 Latest: 2.10.0	NTSC/ PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	No	No	NA
2500 Series	Minimum: 2.5.2.2	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	NA
2600 Series	Minimum: 4.4.2	NTSC / PAL	H.264 MJPEG -4 MJPEG	Yes	Yes	Yes	Yes	No	No	NA
2830	Minimum: 2.0.3 Latest: 2.12.22.12.2	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
2835	Minimum: 2.0.3 Latest: 2.12.2	PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
2900 Series	Minimum: 1.6.8	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	NA

1. The **minimum firmware i**s required for video streaming and recording functionality.

Table 4 Cisco 3000 Series

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
3050	Minimum: 2.6.0 Latest: 2.12.2	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0
3421V	Minimum: 2.0.3 Latest: 2.10.0	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	2.5.0
3520	Minimum: 2.0.3 Latest: 2.10.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0

Table 4 Cisco 3000 Series

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
3530	Minimum: 2.0.3 Latest: 2.12.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
3535	Minimum: 2.0.3 Latest: 2.10.0	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
3620	Minimum: 2.7.1 Latest: 2.12.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0
3630	Minimum: 2.7.1 Latest: 2.12.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

Table 5 Cisco 4000 Series and 5000 Series

Basic functionality such as streaming and recording is supported. Any features that require a firmware upgrade are not supported.

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
4300	Minimum: 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A
4300E	Minimum: 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A
4500	Minimum: 2.4.2-289	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A
4500E	Minimum: 3.2.3-218	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No	No	N/A
5000 Series	Minimum: 1.6.17	NTSC	H.264 MJPEG	NA	Yes	Yes	Yes	No	No	N/A

1. The **minimum firmware is** required for video streaming and recording functionality.

Table 6 Cisco 6000 Series

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
6000P	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
6020	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
6030	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
6050	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	Yes	Yes	2.5.0
6400	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
6400E	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
6500PD	Minimum: 2.5.1 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.1
6620	Minimum: 2.7.1 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0
6630	Minimum: 2.7.1 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0
6930	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

Table 7 Cisco 7000 Series

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Min. FW Version
7030	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
7030E	Minimum: 2.0.3 Latest: 2.12.6-5	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.0
7070	Minimum: 2.6.0 Latest: 2.12.6-5	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.7.0
7530PD	Minimum: 2.5.1 Latest: 2.12.6-5	NTSC/ PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes	2.5.1

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

Table 8 Cisco 8000 Series

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types[2]	Dual Stream	Motion Detection[3]	Firmware Upgrade	Privacy Mask[4]	Edge Storage	Audio	Camera App Support[5]
8020	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8030	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8070	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8400	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes

Table 8 Cisco 8000 Series (continued)

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types[2]	Dual Stream	Motion Detection[3]	Firmware Upgrade	Privacy Mask[4]	Edge Storage	Audio	Camera App Support[5]
8620	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8630	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8930	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes
8000P	Minimum: 1.0.2 Latest: 1.0.9-18	NTSC/ PAL	H.265 / H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes G.711 pcmu	Yes

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Camera mode SHOULD be 5MP while adding to VSOM to support all resolutions.
3. Five window video motion detection.
4. Privacy Mask will be enabled until user d2.12.6-5isables it from VSOM, unlike earlier CISCO cameras where Privacy Mask used to get disabled after privacy mask timer is elapsed.
5. Camera apps feature of Cisco 8xxx series camera will work with firmware version 1.0.9-9 only.

Table 9 Cisco CIVS-SENC-4P and CIVS-SENC-8P

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade	Privacy Mask	Edge Storage	Camera App Support
CIVS-SENC-4P (encoder)	Minimum: V1.2.0-4	NTSC/ PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No	No	No
CIVS-SENC-8P (encoder)	Minimum: V1.2.0-4	NTSC/ PAL	H.264 MPEG-4 MJPEG	Yes	NA	Yes	Yes	No	No	No

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

Additional Notes on Cisco Devices

- Cisco 4500 and 4500E support video analytics.
- Cisco 5000 series does not support motion detection at video bit-rates above 4,000 (4 Mbps). The “H” video preset in Templates has been chosen to not exceed this, so motion detection will work.

- The Cisco 5000 and 2900 camera series do not allow changes to the authentication settings (username/password) or networking settings (DHCP/Static, DNS, etc.) through Cisco VSM. These values can only be changed using the camera web interfaces.
- Focus, Auto Focus and Zoom support are not available for Cisco 6000P, 3421V, 3520, 3530, 3535, and 3050 camera models.
- When Cisco 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.
- Cisco 3421V and 6050 cameras do not support Contact Closure, Cisco 7030 camera supports 3 input ports. All other Cisco 3000, 6000, 8000 series cameras support 1 input port.
- In PTZ Tour Configuration, the configured transition time configured includes the time that it takes the camera to move from the 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.
- The minimum firmware version required to support camera applications is 2.5.0-10.
- The minimum firmware version required to support connected edge storage is 2.0.

Supported Devices: Arecont

Table 10 provides information about Arecont devices that this Cisco VSM release supports.

Table 10 Supported Arecont Cameras

Model	Type	Supported FW Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV2115	2MP IP Camera	65218	H.264 MJPEG	Yes	Yes	No
AV5155	5MP IP Camera	65152	H.264 MJPEG	Yes	Yes	No
AV5115	5MP IP Camera	65220	H.264 MJPEG	Yes	Yes	No
AV10XX5	10MP IP Camera	65218, 65202	H.264 MJPEG	Yes	Yes	No
AV8185DN	4 Sensor 2MP Panoramic IP Camera	65183, 65192	H.264 MJPEG	Yes	Yes	No
AV8365DN	4 Sensor 2MP Panoramic IP Camera	65170	H.264 MJPEG	Yes	Yes	No
AV12186DN	4 Sensor 3MP Panoramic IP Camera	65184	H.264 MJPEG	Yes	Yes	No

Table 10 Supported Arecont Cameras (continued)

Model	Type	Supported FW Version	Media Types	Dual Stream	Motion Detection	Firmware Upgrade
AV20365DN	4 Sensor 5MP Panoramic Camera	65170	H.264 MJPEG	Yes	Yes	No
AV20185DN	4 Sensor 5MP Panoramic Camera	65183, 65200	H.264 MJPEG	Yes	Yes	No

Additional Notes on Arecont Devices

- AV20185, AV20365, AV12186, AV8365 and AV8185 are 4-channel IP cameras. In order to support multiple video channels from a single device, Cisco VSM 7 models these devices as “Encoders”.
- Arecont devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Secondary streams are not supported in H, M, L template settings for Arecont Devices. However secondary stream can be configured using Custom templates.
- Arecont cameras divide the Maximum FPS the camera supports by the number of streams. This could result in lower FPS when both primary and secondary streams are configured for these cameras.
- Arecont AV10XX5, AV5115, AV2115 support VBR and multicast streaming.
- There is a restriction with motion detection for Arecont multi-sensor cameras. False motion events are generated if both half and full resolution size images are requested simultaneously using Cisco VSM or Arecont Camera Web Interface or a third party Media Player.

Supported Devices: Axis

Table 11, Table 12, and Table 13 provide information about Axis devices supported in this release.

Table 11 Supported Axis Cameras

Model	Type	Supported Firmware Version[1]	Video Format	Media Types	Video Ports	Dual Stream	Motion Detection	Max Motion Window	Audio	PTZ
Q6000-E	Encoder	6.40.1	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	10	No	No
P3717-PLE	Encoder	9.40.1	NTSC/PAL	H264/ MJPEG	4	Yes	Yes	10	No	No
P3707-PE	Encoder	6.50.1.3	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	10	No	No
Q6052-E	IP Camera	7.20.1	NTSC/ PAL	H264/ MJPEG	1	Yes	Yes	10	No	Yes

Table 11 Supported Axis Cameras (continued)

P1428E	IP Camera	6.50.2	NTSC/ PAL	H264/ MJPEG	1	Yes	Yes	10	No	No
Q1659	IP Camera	6.56.1	NTSC/ PAL	H264/ MJPEG	1	Yes	Yes	10	Yes	No

1. The minimum firmware is required for video streaming and recording functionality. The latest firmware may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.

Table 12 Supported Axis Encoders

Model	Type	Supported Firmware Version[1]	Video Format	Media Types	Video Ports	Dual Stream	Motion Detection	Audio	Firmware Upgrade	Zoom to Region
P7224	Encoder	5.51.2.7	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	Yes	Yes	No
P7216	Encoder	5.51.6	NTSC/ PAL	H264/ MJPEG	16	Yes	Yes	Yes	Yes	No
Q7424-R MK II	Encoder	5.51.3.2	NTSC/ PAL	H264/ MJPEG	4	Yes	Yes	Yes	Yes	No
Q7436	Encoder	6.30.1	NTSC/ PAL	H264/ MJPEG	6	Yes	Yes	No	Yes	No

1. The minimum firmware is required for video streaming and recording functionality. The latest firmware may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the encoder model and firmware version.

Table 13 provides information about additional Axis devices that this Cisco VSM release supports.

Table 13 Additional Supported Axis Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade	Zoom to Region
233D	IP Camera	4.48.4	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
243SA	Encoder	4.45	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
241Q	Encoder	4.47.5	NTSC PAL	MPEG-4 MJPEG	No	Yes	Yes	Yes	Yes	No
241S	Encoder	4.40	NTSC PAL	MPEG-4 MJPEG	No	Yes	Yes	Yes	Yes	No
243QBlade	Encoder	4.46.1	NTSC / PAL	MPEG-4 MJPEG	NA	Yes	Yes	Yes	Yes	No
247S	Encoder	4.42	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No

Table 13 Additional Supported Axis Devices (continued)

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade	Zoom to Region
F44	Encoder	6.50.1.2	NTSC / PAL	MPEG-4 MJPEG	Yes	Yes	Yes	Yes	Yes	No
M3006	IP Camera	5.55.1.2	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No
M3007	Panoramic Camera	5.40.13.2	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No
P1214	IP Camera	5.40.12.3	NTSC	H.264 MJPEG	No	Yes	Yes	Yes	Yes	No
P1353	IP Camera	5.40.19.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3301	IP Camera	5.40.92	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3364	IP Camera	5.40.17.1	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3367	IP Camera	6.50.1.3	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P3915	IP Camera	5.55.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
P7214	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q1604	IP Camera	5.50.3	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q3708	IP Camera	5.95.4.1	NTSC/ PAL	H264/ MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q6045	IP Camera	5.55.11	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes
Q7401	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q7404	Encoder	5.50.2	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes
Q7406	Encoder	5.11.1	NTSC / PAL	H.264 MJPEG	N/A	Yes	Yes	Yes	Yes	Yes
Q7424	Encoder	5.50.02	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	Yes	Yes
Q3617-VE	IP Camera	9.30.1	NTSC/ PAL	H264/ MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q3615-VE	IP Camera	9.30.1	NTSC/ PAL	H264/ MJPEG	Yes	Yes	Yes	Yes	Yes	No
Q8742-E	IP Camera	7.15.4.1	NTSC/ PAL	H264/ MJPEG	Yes	Yes	Yes	Yes	Yes	No

Additional Notes on Axis Devices

- Axis P3301 IP camera and Q7401, Q7404, and Q7406 encoders have been qualified to support redundancy in Cisco VSM 7.0.1.
- Axis 233D supports contact closure configuration and events.
- Support for 0.1fps MJPEG stream for all supported Axis models.

The following table documents the various Field-Of-Views supported for the Axis M3007 panoramic cameras and support for PTZ and Motion Detection for these Field-Of-Views.

Table 14 Axis M3007,M3037 Options

Model	Field Of View	PTZ	Motion Detection
Axis M3007 Axis M3037	360° view	No	Yes
	Panoramic view (180 degree view)	No	No
	Double Panoramic view(2 panoramic view of 180 degree)	No	No
	Quad view (view area 1,2,3,4)	No	No
	View Area 1	Yes	No
	View Area 2	Yes	No
	View Area 3	Yes	No
	View Area 4	Yes	No

The Axis M3007 and M3037 camera allows the user to configure various mounting options directly in the camera web interface that affects the possible values for Field-Of-Views that can be configured on the camera. The table below provides this mapping:

Table 15 Axis M3007 and Axis M3027 Field-Of-View Options

Field of View / Mount Point	Wall	Ceiling	Desktop
360 Degree View	Yes	Yes	Yes
Panoramic View	Yes	Yes	Yes
Double Panoramic View	No	Yes	Yes
Quad View	No	Yes	Yes
View Area 1/2/3/4	Yes	Yes	Yes

Supported Devices: IQinVision

Table 16 provides information about IQinVision devices that this Cisco VSM release supports.

Table 16 Supported IQinVision Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Stream Mirroring	Motion Detection	Firmware Upgrade
IQ032SI-V11	IP Camera	V3.4/5	NTSC	H.264	No	No	No	Yes	Yes
IQM32NE-B5	IP Camera	V3.4/5	NTSC	H.264	No	No	No	Yes	Yes
IqeyeA35N	IP Camera	V3.4/5	NTSC	H264	No	No	No	Yes	Yes
Iqeye765N	IP Camera	V3.4/5	NTSC	H264	No	No	No	Yes	Yes
Iqeye755	IP Camera	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes

Additional Notes on IQinVision Devices

- IQinVision devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Support configuring NTP on the IQinVision cameras to synchronize with their Cisco VSM Media Server.
- Added support for Firmware upgrade for all supported models.
- Added support for Camera Discovery for H.264 models.

Supported Devices: Mobotix

Table 17 provides information about Mobotix devices that this Cisco VSM release supports.

Table 17 Supported Mobotix Devices

Model	Type	Supported FW Version	Video Format	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
x10	IP Camera	MX-V4.x	NTSC	MPEG-4 MJPEG	No	No	No	No

Additional Notes on Mobotix Devices

- Moboitx M10 and D10 IP cameras running with M10 series firmware work with the x10 Model.
- Mobotix devices are not qualified to support redundancy in Cisco VSM 7.

Supported Devices: Panasonic

Table 18 provides information about Panasonic devices that this Cisco VSM release supports.

Table 18 Supported Panasonic Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
NP 244	IP Camera	1.80 E4	NTSC	MPEG-4 MJPEG	NA	No	Yes	No
NS 202A	IP Camera	2.74P0	NTSC	MPEG-4 MJPEG	No	No	Yes	No
NP 304	IP Camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No
SW 458	Panoramic Camera	1.42	NTSC	H.264, MJPEG	No	Yes	Yes	No
SF 438	Panoramic Camera	1.42	NTSC	H.264, MJPEG	No	Yes	Yes	No
NF 302	IP Camera	1.64E0_1.06	NTSC	MPEG-4 MJPEG	No	No	Yes	No

Additional Notes on Panasonic Devices

- Panasonic devices have not yet been qualified to support redundancy in Cisco VSM 7.
- Only same field of views can be configured on primary and secondary streams on Panasonic cameras SW458/SF438.
- The following table documents the various Field-Of-Views supported for the Panasonic SF 458 and SF 438 panoramic cameras and support for PTZ and Motion Detection for these Field-Of-Views.

Table 19 Panasonic SF 458 and SF 438 Field-Of-Views Support

Model	Field Of View	PTZ	Motion Detection
Panasonic SW458 and SF438	Panoramic 360 degree view	No	Yes
	Double Panorama view(2 panoramic view of 180 degree)	No	Yes
	Panorama view (180 degree view)	No	Yes
	Quad view	No	No
	Single view	Only with View Area 1	No

Supported Devices: Pelco

Table 20 provides information about Pelco devices that this release supports.

Table 20 Supported Pelco Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
Pelco ExSite	IP Camera	TXB-N-1.9.2.12-20131118-1.2084-O1.10263	NTSC, PAL	H.264, MJPEG	No	Yes	Yes	Yes
Pelco Spectra IV TXB IP (MPEG4)	IP Camera	01.02.0018	NTSC	MPEG4, MJPEG	No	Yes	No	No
Pelco NET5404T	Encoder	1.8.2.18-20121109-1.3081-O3.8503	NTSC, PAL	H.264, MJPEG	Yes	Yes	Yes	No
Pelco NET5401T	Encoder	1.9.2.1-20130619-3.3081-O3.9819	NTSC, PAL	H.264, MJPEG	Yes	Yes	Yes	No

Additional Notes on Pelco Devices

- Pelco devices have not yet been qualified to support Redundancy in Cisco VSM 7.
- Audio volume controls are not supported for NET540XT
- For Pelco NET540xT PTZ to work, the analog camera should be chosen as Pelco Analog Camera (pelco_sarix) in Operations Manager and not as Pelco D.
- The user needs to directly configure the Serial protocol on the Pelco NET540XT encoder outside of Cisco VSM.
- The Pelco Spectra IV TXB-N (H.264 capable model) run Pelco Sarix firmware and can be supported in Cisco VSM as a Pelco Sarix Generic IP camera (additional details in the Generic IP camera section).

Supported Devices: Sony

Table 21 provides information about Sony devices that this release supports.

Table 21 Supported Sony Devices

Model	Type	Supported FW Version	Video Formats	Media Types	Audio	Dual Stream	Motion Detection	Firmware Upgrade
HM662	Panoramic Camera	1.1.1	NTSC / PAL	H.264 MJPEG	No	Yes	No	No
RX 530	IP Camera	3.15	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No

Table 21 Supported Sony Devices (continued)

RX 570	IP Camera	3.15	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No
RX 550	IP Camera	3.14	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	No	Yes	No

Additional Notes on Sony Devices

- Sony devices have not yet been qualified to support redundancy in Cisco VSM 7.
- These Sony devices do not support motion detection with the H.264 media type.
- The Sony SNC-RX5x0 cameras stop streaming video when the Object Detection window is opened in the camera's web interface.
- For Sony HM662 Panoramic camera, only the 360 degree view is supported. De-warped views are not supported.

Supported Devices: Vivotek

Table 22 provides information about Vivotek devices that this release supports.

Table 22 Vivotek

Model	FW Version for Release 7.14 Compatibility[1]	Video Format	Media Types	Dual Stream	Motion Detection[2]	Firmware Upgrade	Privacy Mask	Edge Storage	Audio	Contact Closure
SD9361-EHL	Latest: 0102f	NTSC/ PAL	H.265/ H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	Yes
SD9362-EH/ SD9362-EHL	Latest: 0102f	NTSC/ PAL	H.265/ H.264 MJPEG	Yes	Yes	Yes	No	No	Yes G.711 pcmu	Yes

1. The **minimum firmware i**s required for video streaming and recording functionality. The **latest firmware** may be required to support new features, as indicated in the feature columns or descriptions. For more information, including caveats and supported features, see the release notes for the camera model and firmware version.
2. Five window video motion detection.

Supported Devices: Generic IP Cameras

Cisco VSM Release 7.14 provides the following device drivers to support IP cameras from various vendors. The functionality they support will depend on the particular device that they are used with. They are intended to provide a quick and easy way to support devices for which there isn't yet a specific driver available for Cisco VSM. Since these drivers may not be tested with a specific device, some issues may be encountered. When using these drivers with a device, failover and redundancy are not supported.

Note The vendor specific generic driver should always be used before a non-vendor specific driver such as ONVIF.

Table 23 Supported Generic Devices

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection [1]	Firmware Upgrade
Arecont	Arecont Non Panoramic Models	NTSC	H.264 MJPEG	No	Yes	No	Yes	No
Bosch Generic	CPP4 - 6.22 CPP7 - 6.30	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	No
Bosch Panoramic	CPP4 - 6.22	NTSC	H.264 MJPEG	Yes	Yes	Yes	Yes	No
Generic Axis	3.0 / Firmware 5.x	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No
Generic Axis	2.0 / Firmware 4.3	NTSC / PAL	MPEG4 MJPEG	Yes	Yes	Yes	Yes	No
IQEye H264	V3.4/5	NTSC	H264 MJPEG	No	Yes	No	Yes	Yes
IQEye JPEG	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
Mobotix	MX Series	NTSC / PAL	MJPEG	No	No	No	Yes	No
ONVIF	2.2	NTSC / PAL	H.264 MPEG-4 MJPEG	Yes	Yes	Yes	Yes	No
Panasonic	-	NTSC / PAL	H.264 MPEG-4 MJPEG	No	Yes	Yes	Yes	No

Table 23 Supported Generic Devices (continued)

Type	Supported Version	Video Formats	Media Types	Audio	Dual Stream	PTZ	Motion Detection [1]	Firmware Upgrade
Pelco Sarix	Only IP cameras with Sarix Firmware	NTSC / PAL	H.264 MJPEG	No	Yes	Yes	Yes	No
Sony	6th Generation IP cameras VMxxx and VBxxx	NTSC / PAL	H.264 MJPEG	Yes	Yes	Yes	Yes	No
Sony	2nd, 3rd, 4th and 5th generation Sony IP cameras	NTSC / PAL	H.264, MPEG-4, MJPEG	Yes	Yes	Yes	Yes	No

1. Only ONVIF cameras manufactured by Samsung, and Vivotek support motion detection. Motion windows must be configured directly on the camera using the camera UI before the camera is configured using Cisco VSM.

Known Limitations

- Supports only IP Cameras, no support for Encoders
- No contact closure support
- Multicast streaming is supported only for the primary stream
- Multicast port must be an even number within the range 16000:19999
- Audio Multicast issues are observed on most of the ONVIF cameras. Hence do not enable audio when multicast is enabled for video.
- Capture Mode on the camera cannot be changed using ONVIF APIs. So, it is assumed that the camera is in the desired capture mode before adding it to VSOM using ONVIF

Device Specific Limitations

- This ONVIF driver has been tested with a limited number of camera models from Axis, Sony, Panasonic, Bosch, Pelco, Samsung, J2000IP, and Cohu. We have found that these cameras have some variations in how they have implemented the ONVIF specification. Hence there may be compatibility issues when using this ONVIF driver with a particular device that is ONVIF compliant.
- Some of the known caveats are listed below:

AXIS

- ONVIF user account—Some Axis cameras require a special ONVIF user account, which can be created on the camera's web interface before adding an AXIS ONVIF camera to the VSOM. This page is at **Setup --> System Options --> Security --> ONVIF --> Add**
- Camera and VSMS (Media Server) Time Synchronization—ONVIF camera and VSMS server to which ONVIF camera is being added should have their time synchronized ideally using NTP.

SAMSUNG

- Megapixel Mode setting on the camera SND-7080

- To support the resolutions (1600*1200) and (2048*1536), change the Megapixel Mode to 3-Megapixel in the following page on the camera browser: **Settings -> Audio & Video -> video profile -> Megapixel mode**

COHU

- Enable Authentication on the camera before adding it to VSOM in the camera browser, go to **Camera Setup -> Configuration -> User Settings**. Select **User** and enable “Require Password” field.
- Media Transport Type— Only UDP is supported. Streaming fails if TCP is selected.
- Unsupported Resolutions —Streaming fails for the resolutions 176*144, 176*120, 160*120
- Codec Change through VSOM— Switching from H264 to JPEG or vice-versa requires a camera reboot. And camera needs to be deleted and added in VSOM after camera is up.
- Support for Audio— Camera does not support ONVIF Audio

BOSCH

- Frame rate— Only Framerate 30 is supported
- Dual Streaming— Secondary configuration overwrites the primary configuration. So, dual streaming is not supported on Bosch cameras using ONVIF.

PANASONIC

- Capture Mode Setting— If the camera is added in VSOM using Multicast, changing the capture mode on the camera browser manually causes the streaming to fail. After this, only the unicast streaming works
- User Authentication— User Authentication should be enabled in the camera browser as follows - **Setup -> User mng -> User auth**. Choose **ON** for User auth.

SONY

- Media Transport Type— Only UDP is supported. Streaming fails if TCP is selected
- Support for Audio— Camera does not support ONVIF Audio
- Set Configuration Issues — Camera returns success even if one or more of the parameters are not valid for that camera/video stream. ONVIF profile gets updated with values but Camera still uses the previous correct value. Recommend to configure only the values as allowed in the camera browser.
- Support for Password change on the camera— Camera does not support password change for the administrator users using ONVIF API.

Supported Devices: Analog Cameras

This Cisco VSM release provides support for the following analog cameras.

Table 24 Supported Devices: Analog Cameras

Type	Video Formats	Serial Protocol Support
Generic	NTSC / PAL	No
Axis Analog Camera	NTSC / PAL	Encoder dependent: use the encoder's PTZ driver. For use with Axis VAPIX 3.0 video encoders
Bosch	NTSC / PAL	Yes
Panasonic	NTSC / PAL	Yes
Generic Pelco-D	NTSC / PAL	Pelco-D
Generic Pelco P	NTSC / PAL	Pelco P
Pelco Min-Spectra	NTSC / PAL	Pelco-D
Pelco Analog Camera	NTSC / PAL	Encoder Dependent (for use with only PelcoNET540xT encoders)
Cyberdome I	NTSC	Yes
Cyberdome II	NTSC	Yes

Notes on Cyberdome devices

- The Cyberdome I and Cyberdome II devices also have On Screen Display Menu support.

Device Models Validated in Cisco VSM as Generic IP Cameras

The camera models listed in Table 25 have been tested with VSM Release 7.14 as generic IP cameras.

Table 25 Supported Generic IP Cameras

Model	Type	Firmware	Format	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
Arecont AV1355	Arecont	65151	NTSC / PAL	H.264	No	Yes	No	Yes	No
Arecont AV3115	Arecont	65218	NTSC / PAL	H.264	No	Yes	No	Yes	No
Axis 215	Axis VAPIX 2.0 /Firmware 4.3	4.48.4	NTSC / PAL	MPEG4, MJPEG	Yes	Yes	Yes	Yes	No
Axis 3301	Axis VAPIX 3.0/Firmware 5.x	5.41.2	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	Yes	No
Axis 3367	Axis VAPIX 3.0/Firmware 5.x	6.10.1	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	Yes	No
Axis Q6034	Axis VAPIX 3.0/Firmware 5.x	5.41.1.2	NTSC / PAL	H.264, MJPEG	Yes	Yes	Yes	Yes	No
Axis Q6034-E	ONVIF 2.0	5.41.1.2	NTSC	H.264, MJPEG	Yes	Yes	Yes	No	No
Axis Q6045	ONVIF 2.2	5.55.1.1	NTSC	H.264, MJPEG	No	Yes	Yes	No	No
Bosch FLEXIDOME IP 7000MP Panoramic	Bosch Panoramic	6.22.0007	NTSC	MPEG4, MJPEG	Yes	Yes	No	No	No
Bosch FLEXIDOME IP dynamic 7000 VR	Bosch Generic	5.93.0025	NTSC	MPEG4, MJPEG	Yes	Yes	No	No	No
Bosch FLEXIDOME IP outdoor 5000 HD	Bosch Generic	6.22.0007	NTSC	MPEG4, MJPEG	No	Yes	No	Yes	No
Bosch FLEXIDOME IP starlight 6000 VR	Bosch Generic	6.30.0139	NTSC	MPEG4, MJPEG	Yes	Yes	No	No	No
IQinVision IQ755	IQEye JPEG	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQinVision IQ853	IQEye Jpeg	V3.1/2	NTSC	MJPEG	No	No	No	Yes	Yes
IQinVision IQA35N	IQEye H264	V3.4/6	NTSC	H.264, MJPEG	No	Yes	No	Yes	Yes

Table 25 Supported Generic IP Cameras (continued)

Model	Type	Firmware	Format	Media Types	Audio	Dual Stream	PTZ	Motion Detection	Firmware Upgrade
IQinVision IQM32N	IQEye H264	V3.4/6	NTSC	H.264, MJPEG	No	Yes	No	Yes	Yes
Panasonic NP-502S	Panasonic	1.81	NTSC / PAL	H.264, MPEG4, MJPEG	No	Yes	No	Yes	No
Panasonic SC384	Panasonic	1.44	NTSC / PAL	H.264, MJPEG	No	Yes	Yes	Yes	No
Panasonic SF538	ONVIF 2.1.1	1.31	NTSC	H.264, MJPEG	No	Yes	No	No	No
Panasonic SW458	ONVIF 2.0	1.42	NTSC	H.264, MJPEG	Yes	Yes	No	No	No
Panasonic SW458	Panasonic	1.42	NTSC / PAL	H.264, MJPEG	No	Yes	Yes	Yes	No
Pelco IDS0DN-AD AURX7	Pelco	1.8.2.20-20130211-2.9110-03.9240	NTSC	H.264, MJPEG	No	Yes	No	Yes	No
Pelco ISXOC	Pelco	1.9.2.2-20130717-1.9080-A1.9926	NTSC	H.264, MJPEG	No	Yes	No	Yes	No
Samsung SND-7080	ONVIF 2.1.0	1.10_110819	NTSC	H.264, MJPEG	No	Yes	No	No	No
Samsung SND-7080	ONVIF 2.0	2.00_121004	NTSC	H.264, MJPEG	No	Yes	No	No	No
Sony CH 240	Sony 2nd, 3rd, 4th and 5th generation Sony IP cameras	1.79.00	NTSC / PAL	H.264, MPEG4, MJPEG	Yes	Yes	No	Yes	No
Sony CH180	ONVIF 2.2	1.34.00	NTSC	H.264, MJPEG	Yes	Yes	No	No	No
Sony VM 631	Sony 6th Generation IP cameras VMxxx and VBxxx	1.3.0	NTSC / PAL	H.264, MJPEG	Yes	Yes	No	No	No

Clipping Support By Application

You can create and view video clips using the following Cisco VSM applications:

Table 26 Video Clip Support

Application	Create MP4 Clips	Create CVA Clips	Create Virtual Clips	View MP4 Clips[1]	View CVA Clips	View Virtual Clips	Clip Search Feature
Cisco VSM Operations Manager	Yes	Yes	Yes	Yes	No	Yes	Yes
Cisco VSM Federator	Yes[2]	Yes	No	Yes[3]	No	Yes[4]	Yes
Cisco SASD	Yes	Yes[5]	Yes[6]	Yes	No	Yes	Yes
Cisco SASD Federator	Yes	Yes	Yes[7]	Yes	No	Yes	Yes
Cisco VSM Review Player	No	No	No	Yes	Yes[8]	No	No

1. MP4 clips are saved to the Media Server and play immediately after being downloaded to the monitoring PC. Third-party video players (such as VLC media player™) can also be used to view MP4 clips.
2. Create MP4 clips using the Federator Thumbnail Search.
3. Federator clips must be downloaded and played using either Cisco Review Player or VLC.
4. Double-click the virtual clip in Federator Clip Search to launch the player.
5. SASD allows CVA clipping for multi-pane in Sync Mode only.
6. Thumbnail Search supports MP4 clip creation only.
7. Thumbnail Search supports MP4 clip creation only.
8. Cisco video archive (CVA) files can only be opened in applications that support the CVA format (such as the Cisco Review Player).

Note When converting a virtual clip to an MP4 file, only the entire duration of the virtual clip can be saved, not a segment.

Obtaining and Installing Licenses

To install a license, purchase the license and obtain the license file, then upload the file to the Operations Manager.

Table 27 lists the part numbers for the Cisco VSM licenses. Multiple camera and VSMS licenses can be included in a single license file. For example, a single license file might include support for 25 additional cameras and two additional VSMS devices.

Table 27 License Part Numbers

Part	Description
Physical Server Licenses (for Server Services)	
FL-CPS-MS-SW7	License for 1 Media Server on a physical server (Cisco UCS or MSP)
FL-CPS-OM-SW7	License for 1 Operations Manager on a physical server (Cisco UCS or MSP)
L-CPS-MS-SW7=	eDelivery license for 1 Media Server on a physical server (Cisco UCS or MSP)
Virtual Machine (VM) Licenses (for Server Services)	
L-CPS-VSMS7-B-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS B Series
L-CPS-VSOM7-B-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS B Series
L-CPS-VSMS7-C-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS C Series
L-CPS-VSOM7-C-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS C Series
L-CPS-VSMS7-E-VM=	eDelivery license for one Media Server on a VM running on a Cisco UCS E-Series
L-CPS-VSOM7-E-VM=	eDelivery license for one Operations Manager on a VM running on a Cisco UCS E-Series
Cisco VSM Federator Licenses	
L-CPS-VSM7-FD=	eDelivery license for one base Cisco VSM 7 Federator
L-CPS-FD-VSOM=	eDelivery license for one Operations Manager in Federator
L-CPS-FD-VSOM-X=	eDelivery license for one Operations Manager Express in Federator
Cisco SASD Licenses	
L-CPS-SASD-7=	eDelivery license for 1 SASD with Cisco VSM 7
Camera Licenses	
L-CPS-VSM7-1CAM=	eDelivery license for 1 camera connection with Cisco VSM 7
Camera App Licenses **Note** The following licenses are used when managing Camera Apps using Cisco VSM Operations Manager. These licenses are different than those used when installing and managing the Camera Apps directly on the device (using the device UI).	
L-FL-IVVA-T1-VSM=	Tier 1 Cisco IP Camera Intuvision Video Analytic App for VSM

Notes

- A license for 10,000 Cisco cameras is included by default (you do not need to purchase and install an additional license for Cisco cameras).
- You can add 1 Media Server and 10 non-Cisco cameras without a license for initial setup purposes only. This feature is removed when you add any permanent license.

Procedure

Step 1 Purchase additional licenses:

a. Determine the part number for the license you want to purchase (see Table 27).

b. Purchase the license by contacting your Cisco sales representative or any Cisco reseller. For more information, visit http://www.cisco.com/en/US/ordering/index.shtml.

c. When the purchase is complete, you are issued a Product Authorization Key (PAK) in paper form, or in an e-mail message.

Step 2 Obtain the license file:

a. Locate the Product Authorization Key (PAK) that was created with the purchase.

b. In a web browser, open the Cisco Product License Registration web page.

http://www.cisco.com/go/license/

c. Follow the on-screen instructions to complete the form and enter the Product Authorization Key (PAK). When you are done, a license file with the extension `.lic` is sent to your e-mail address.

d. Transfer the file to the drive of the PC used for the configuration.

Step 3 Install the license file in Cisco VSM:

a. Log in to the Operations Manager.

b. Select **System Settings > Software Licensing**.

c. Click **Add** and select the license file located on your local drive.

d. Click **Save** to install the file and activate the additional capacity.

The additional capacity is available immediately. You do not need to restart the server or take additional steps.

See the Cisco Video Surveillance Operations Manager User Guide for more information.

Understanding the Cisco VSM Software Types

Table 28 describes the different types of software and firmware that are installed on servers, cameras, and encoders.

Table 28 Cisco VSM Software Types

Software Type	Description
System software	System software denotes the Cisco VSM software, including Media Server, Operations Manager, Cisco VSM Management Console, Safety and Security Desktop and Multipane clients. All servers running the Operations Manager and associated Media Server services must run the same software version. Use the Operations Manager to update the *System Software* on all servers (such as Media Servers) associated with the Operations Manager. See the Cisco Video Surveillance Operations Manager User Guide for instructions. **Notes:** • The Operations Manager and all associated servers must run the same system software version. • To update a Federator server, log in to the Federator server Management Console. See the Cisco Video Surveillance Operations Manager User Guide for instructions. • To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager: Install and Upgrade Guide for your hardware platform. For VM installations, see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms).
OVA image (for VM installations)	OVF template files are used to install the system software as a virtual machine (VM) on a supported Cisco Unified Computing System (UCS) platform. • OVA template files are downloaded from the Cisco website. • The file format is `.ova`. For example: `Cisco_VSM-7.12-331d_ucs-bc.ova` • See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for instructions to install the `.ova` image and perform the initial VM setup. • After the VM setup is complete, use the Management Console to complete the configuration.
USB Recovery Disk image	Use the USB Recovery Disk image to create a Cisco VSM 7 Recovery Flash Drive (for example, on a USB stick). The recovery disk can be used do the following: • Repair: reinstalls the Operating System files and partitions without erasing video files stored on the server. You must backup the Cisco VSM database before using the recovery image, and then restore the database after the recovery process is complete. This action also preserves the RAID configuration. • Factory Restore: Restores the server to its factory default settings, reinstalls the operating system, and clears and reconfigures the RAID. This action deletes all data, configurations, software and video files from the appliance, and then reinstalls the operating system and Cisco VSM software. Perform this procedure only if necessary. See the Cisco CSS UCS Server User Guide for more information.
Device *firmware*	Device *firmware* is provided by the device manufacturer. The firmware for Cisco devices can be upgraded using Operations Manager. Firmware for other manufacturers is upgraded using a direct connection. See the “Upgrading Camera and Encoder Driver Firmware” section of the Cisco Video Surveillance Operations Manager User Guide for instructions to upgrade Cisco device firmware, or refer to the device documentation.

Table 28 Cisco VSM Software Types (continued)

Software Type	Description
Device *driver packs*	Device *driver packs* are the software packages used by Media Servers and the Operations Manager to interoperate with video devices, such as cameras. Driver packs are included with the Cisco VSM software, or may be added to a server at a later time to add support for new devices or features. • Install new driver packs to add support for additional devices. • Upgrade existing driver packs to enable support for new features. • When updating or installing a driver pack, you first install the file on the Operations Manager, and then on the Media Servers that support the cameras or encoders. You can install the new version on all Media Servers, or only the Media Server(s) that support the affected devices. If the driver pack version is different on the Media Servers in your deployment, a *driver pack mismatch* error can occur. – A warning message is informational only and the cameras and encoders can be configured normally. – A critical message appears if the driver pack mismatch will impact the functionality or compatibility between the Operations Manager, Media Servers, and the video device. The upgrade is not allowed. Camera and encoder templates cannot be revised until the same driver pack version is installed on all Media Servers. **Note** We strongly recommend upgrading driver packs using the Operations Manager interface (see the "Driver Pack Management" section of the Cisco Video Surveillance Operations Manager User Guide). This allows you to upgrade multiple servers at once.
Language Packs	Language packs can be added to display the Cisco VSM user interfaces in non-English languages. Language packs are added using the Operations Manager (release 7.6 and higher). See the Cisco Video Surveillance Operations Manager User Guide for instructions.

Obtaining Cisco VSM Software

Complete the following procedure to obtain software and other information for the Cisco VSM products and components:

Procedure

Step 1 Go to the Cisco Video Surveillance Manager product page.

Step 2 Click Download Software.

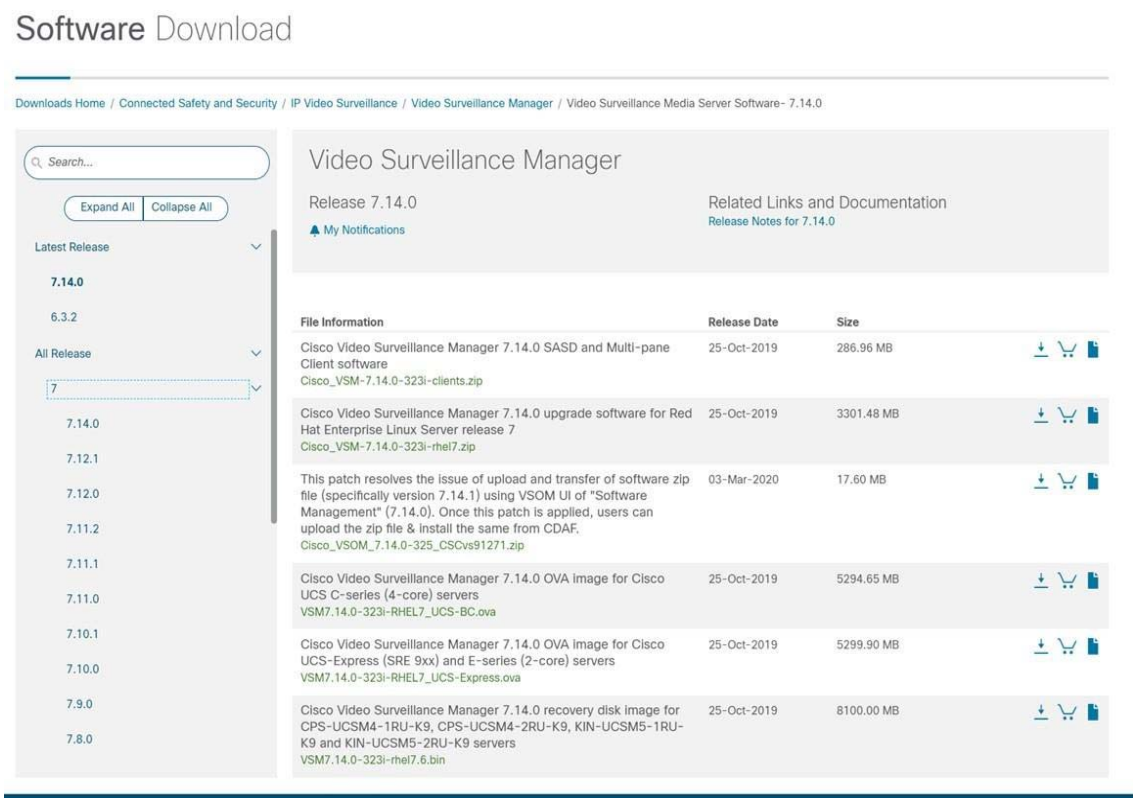
Step 3 Select a product category. For example:

- **Video Surveillance Device Driver**
- **Video Surveillance Manager Stand-alone Tools**
- **Video Surveillance Media Server Software** (including system software)

Step 4 Select the release for your server, device, or deployment (Figure 1).

Step 5 Click **Download** or **Add to Cart** and follow the onscreen instructions.

Figure 1 Download Software Page



Alternate Procedure

You can also navigate the Cisco Physical Security product pages to download software updates and other information:

Step 1 Go to the following URL.

http://www.cisco.com/go/physicalsecurity

Step 2 Click **View All Physical Security Products**.

Step 3 Click **IP Video Surveillance**.

Step 4 Click **Cisco Video Surveillance Manager**.

Step 5 Click **Download Software for this Product**.

Step 6 Click a Software Type and follow the onscreen instructions.

For example: **Video Surveillance Media Server Software** (Figure 1).

Step 7 Select the release for your server, device, or deployment.

Step 8 Click **Download** or **Add to Cart** and follow the onscreen instructions.

Caveats

This section includes the following topics:

Using the Software Bug Search Tool

You can use the Bug Search Tool to find information about most caveats for Cisco VSM releases, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Search Tool, follow these steps:

Procedure

Step 1 To access the Bug Search Tool, 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.

Step 4 For more information, go to the Bug Search interactive tour.

Open Caveats

Table 29 lists caveats that are open in this release.

Caveat	Headline
CSCwd60618	Media server upgrade failed with 'failed to create symbolic link ‘/tmp/tmp’: File exists' error
CSCwd82293	Redundant Pop-up Alert showing up - File not supported, while upgrading to 7.14.7 from CDAF server
CSCwd61839	Redundant Synchronization job internal to upgrade process are failing during upgrade
CSCwd97258	Upgrade to 7.14.7 failed from 7.14.5- Leapp download connection timeout for python3-firewall package
CSCwc73631	Unable to configure Camera App Events on 8k series camera with latest camera app
CSCwe58132	Unable to create Onvif model for Onvif conformant devices
CSCwe84022	User should set Onvif HTTPS port to 443 from Camera UI before adding Infinova as Onvif
CSCwe98260	Motion detection and events not supported on Vivotek-SD-9361-EHL with 0114 firmware
CSCwe98525	Unable to get VideoTag events for 7xxx and earlier camera series.
CSCwf33565	Getting "HA functionality is not available at this time. Pacemaker service is not running" Error
CSCwe70199	Getting load average critical alert for MS performance setup
CSCwf58879	Server import job via csv is getting stopped
CSCwf82805	Load Average Critical Alert on Media Server Performance Setup
CSCwb33782	Intermittent Issue: Pacemaker service is not running while establishing VSOM HA.
CSCwb02957	Communication error while registering VSOM to Smart Licensing server
CSCvu99235	Unable to upgrade VSOM from 7.14.1 to any release between 7.14.2 - 7.14.5 from VSOM UI.
CSCwb13053	Unable to copy latest zip to server's from VSOM UI.
CSCvx98695	Unable to view live/recorded streams if both leader and peer VSOM servers switch to standby.
CSCvx99103	VIP not accessible in VSOM-HA.
CSCvs89900	Unable to upgrade SASD via unattended video wall with “Auto-Upgrade Video Wall” option.
CSCvt34821	Video pane with 360 degree camera cannot be selected in multipane view.
CSCvz58135	Http server core dump created due to MySQL third-party component.
CSCwa10549	Unable to install VMware Tools after upgrading to 7.14.x.
CSCvz92063	Http server core dumps due to “Out of memory” condition by ssl, libstdc++.
CSCvy12474	Error: ums_schema_upgrade-1.0.157.sql - FAILED while restoring Media Server 7.12.0 backup on 7.14.3.
CSCwc73631	Unable to configure Camera App Events on 8K series camera with latest camera app.
CSCwd33426	Firefox browser version 100.0 and above: Unable to view HTML 5 stream.

Troubleshooting Guide for Open Caveats

1. Defect ID: CSCwe98525: System is unable to get VideoTag events for 7xxx and earlier camera series.

Issue:
System is unable to get VideoTag events for 7xxx and earlier camera series. Due to this user will not be able to view events logged under the Camera Events Tab in Camera's status page on VSOM.

Root cause:
This issue arises only when the user inputs a random string (other than "VideoTag") for the TriggerDescription. During configuration, camera mistakenly swaps the values of ‘eventName’ and ‘description’, resulting in an incorrect event being sent to VSM. Consequently, the validation fails, and the event is dropped.

Workaround:
7XXX and earlier camera series being EoS the fix won’t be available. Instead use below steps to correctly generate events for VideoTag app.

When generating VideoTag events through an HTTP POST request, users must input "VideoTag" as the TriggerDescription in the request payload. Any other trigger description will not be allowed.

curl -v -X POST http://IP:PORT -H 'Content-Type: text/xml' --
data '<HttpTrigger><EnableTrigger>1</EnableTrigger><TriggerDescription>VideoTag</TriggerDescription></HttpTrigger>'

Ref:
Refer section ‘Sending an HTTP POST Request Tag Trigger’,
https://www.cisco.com/c/en/us/td/docs/security/physical_security/video_surveillance/ip_camera/camera-apps/8000_series_reference_guide/camera-app-ref/video_tag_app.pdf

---

2. Defect ID: CSCwf33565**:** Add VSOM-HA job completes successfully but system raises critical error on VSOM server.

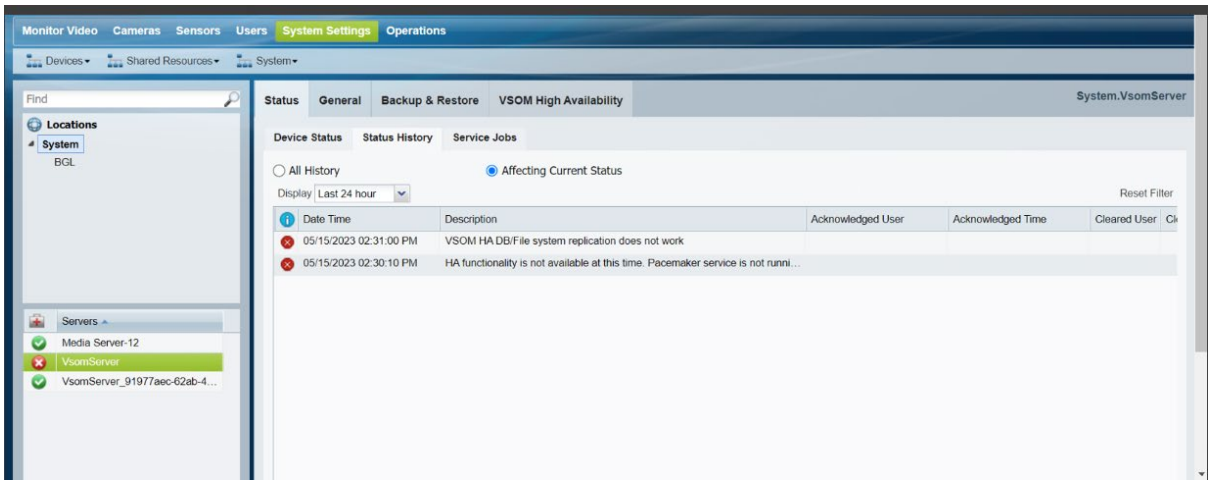
Issue:

Cited critical error is seen on status page of VSOM server that was initially configured as Primary VSOM server, after Add VSOM-HA job completes successfully.

User can login via VIP, but user will observe initial configured Primary VSOM server to be in standby state and initial secondary VSOM server to be in master state.

Root Cause:
Error is reported because initially master server is unable to populate entries for VSOM-HA related tables in the database, however when user performs below workaround the affected server is able to replicate missing data from peer.

Error:
HA functionality is not available at this time. Pacemaker service is not running.



Workaround:

Perform below Steps:

1. Login to CLI of current master VSOM server.

2. Run the below command -

   service pacemaker stop

3. The system will take a while after which the server that was configured initially as Primary will regain master role.

4. Login through VIP and check VSOM High Availability Tab to confirm that master role is acquired mentioned in point 3 above.

5. If status Page of primary VSOM shows critical error "VSOM HA DB/File system replication does not work", then perform "Replace HA"

3. Defect ID: CSCwe84022**:** System fails to add Infinova camera as Onvif

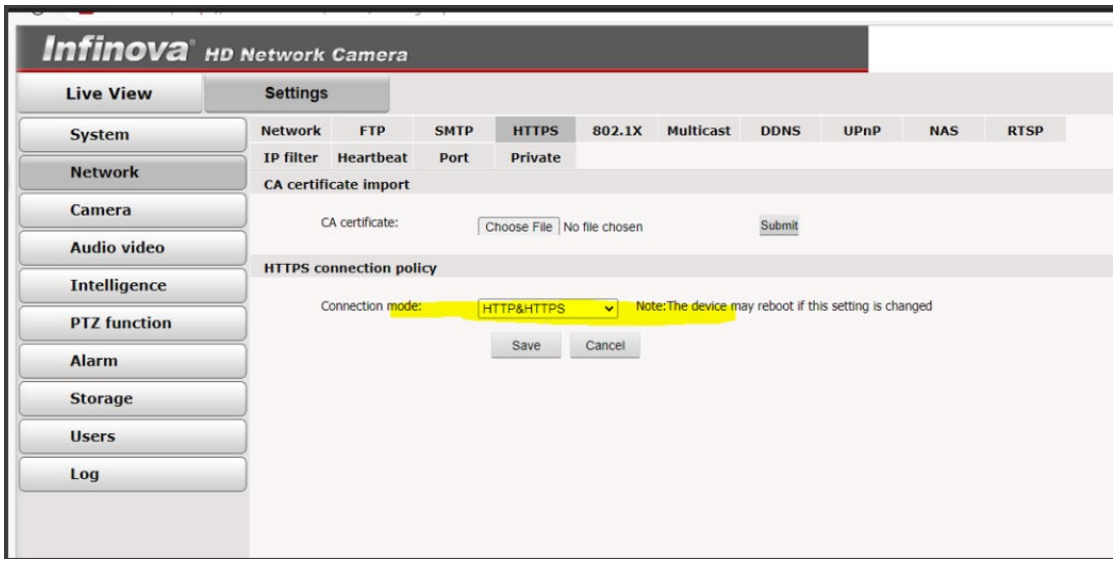
Issue:
System fails to add Infinova camera as Onvif.

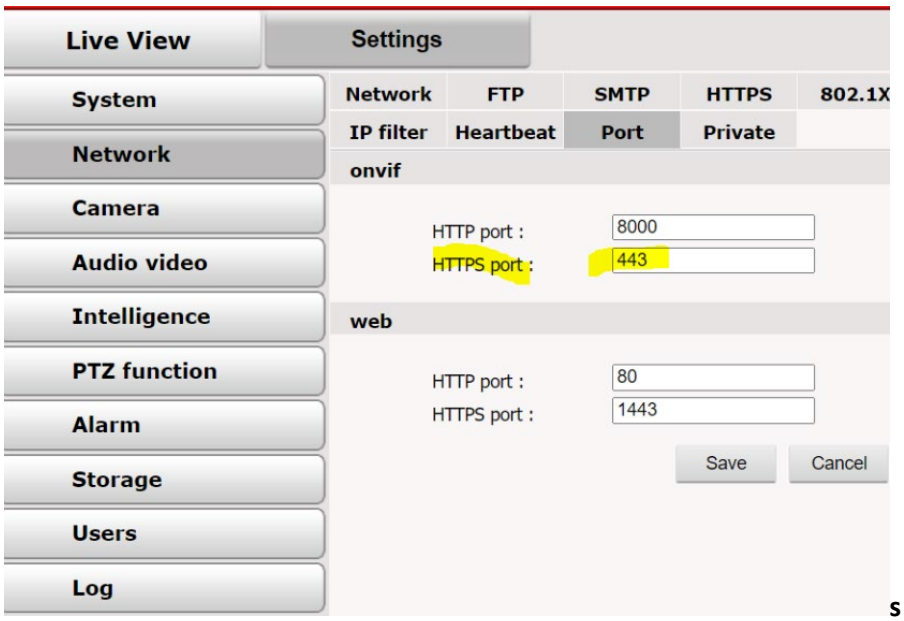
Root cause:
On factory reset, Infinova camera comes with any HTTPS port (Like 1443).
In VSOM, There is no provision of giving custom HTTPS port for Onvif make model while adding camera. VSM by default uses port 443 for Onvif HTTPS communication.
If camera UI has Onvif HTTPS port other than 443, Camera add will fail.

Error:
Invalid username or password or timesync mismatch

Workaround:
For **V4.9.0.201906211448** firmware version: User should set Onvif HTTPS port to 443 from Camera-UI prior to adding camera to VSOM as Onvif model. Also after factory reset, the camera will have "HTTP and HTTPS(Both)" mode enabled. Since VSOM doesn't have provision to assign custom HTTPS port for Onvif camera, the user needs to set Onvif HTTPS port to 443 from camera Ui.

For **V3.4.0.201703271558** firmware version: After factory reset, the camera has HTTP only mode enabled. Here the user doesn't need to set HTTPS port from camera UI.





s

4. Defect ID: CSCwe58132: System fails to create Onvif model for Onvif conformant devices.

Issue:

System fails to create Onvif model for Onvif conformant devices.

Root cause:

During analysis it was found that VSM does not provide the capability to configure NTP and time zone settings. Since product has reached its end-of-life (EOL), no further fixes can be provided.

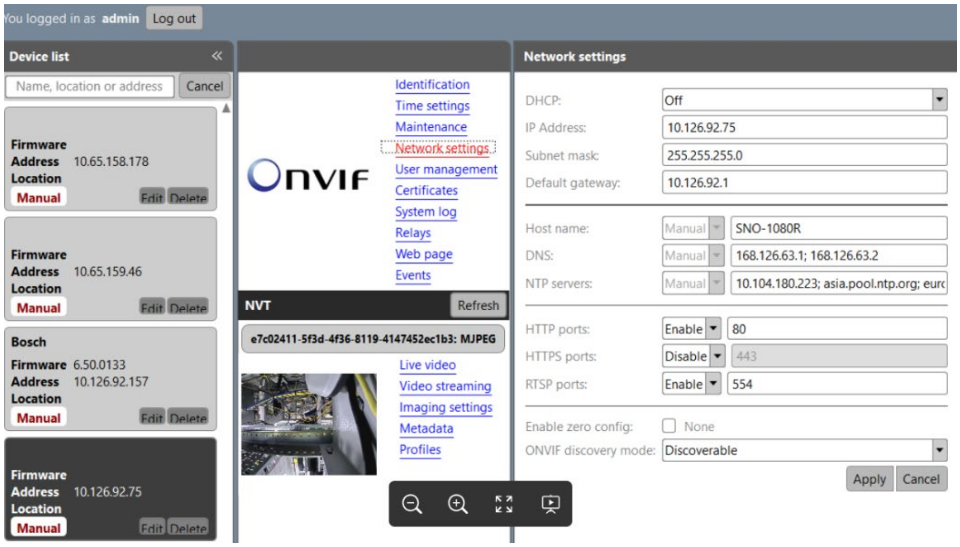
Error:

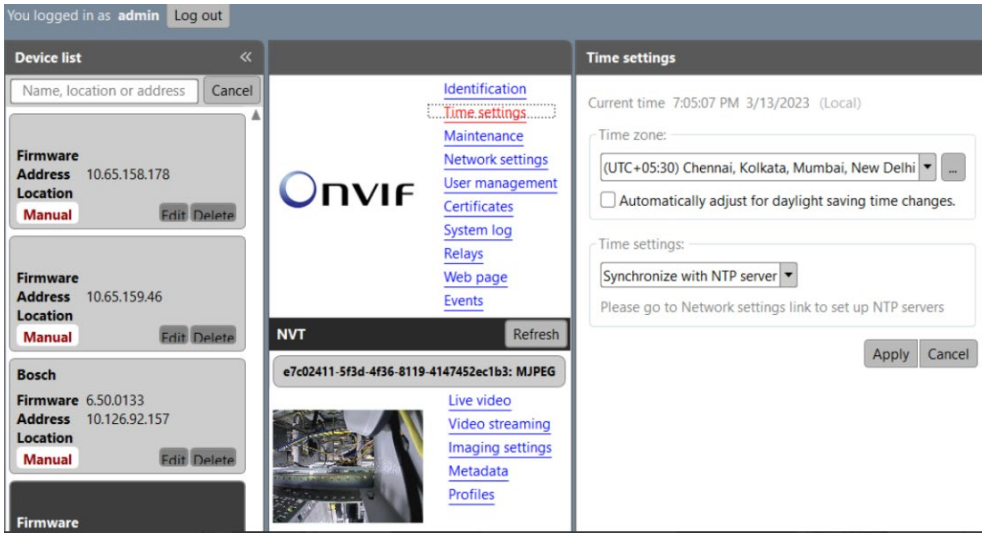
Failed to query device information. GetDeviceCapabilities failed - getDeviceInfo failed to get device information

Workaround:

User should first set NTP and timezone on camera from camera UI and then create Onvif model on VSOM-UI.

In case of Samsung Camera, if UI doesn't open, in spite of installing/updating Webviewer Plugin, user needs to install ODM tool to configure timezone and NTP settings.





5. Defect ID: CSCwe98260: Motion detection and events not supported on Vivotek-SD-9361-EHL with 0114 firmware.

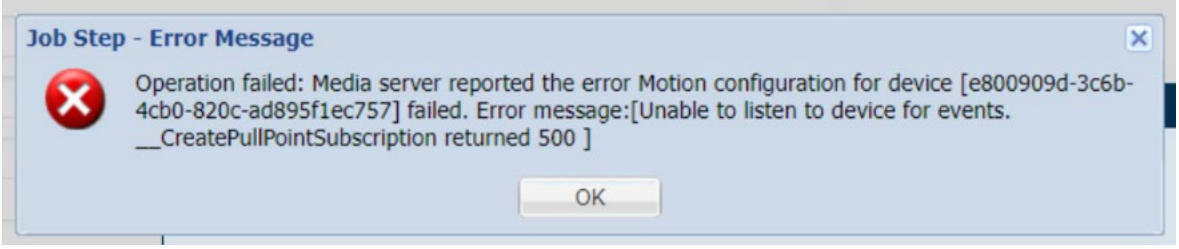
Issue:
Motion detection and events not supported on Vivotek-SD-9361-EHL with 0114 firmware.

Root cause:
VSM supports the following motion format for detecting motion in Onvif-Vivotek cameras:

```
<tt:Message UtcTime="2023-05-17T12:22:02.829Z" PropertyOperation="Changed">
 <tt:Source>
  <tt:SimpleItem Name="Source" Value="VideoSource0"></tt:SimpleItem>
 </tt:Source>
 <tt:Data>
  <tt:SimpleItem Name="State" Value="false"></tt:SimpleItem>
 </tt:Data>
</tt:Message>
```

Any other format for Onvif motion detection is not supported by VSM. It is important to use the specified format mentioned above for proper motion detection integration with Onvif-Vivotek cameras in VSM.

Error:
Media server reported the error Motion configuration for device. Unable to listen to device for events. __CreatePullPointSubscription returned 500



Workaround:
Issue is found to lie on camera's end. No workaround can be provided on VSM. User can attempt to upgrade firmware which supports PullPointSubscription and check if it helps in resolving the issue.

6. Defect ID: CSCwc73631: Unable to configure Camera App Events on 8k series camera with latest camera app.

Issue:
Unable to configure Camera App Events on 8k series camera with latest camera app.
Camera App: Cisco_iV_PN_va_6.0.19.cpk

Root cause:
Issue lies on the camera firmware and not on VSM. Camera throws an error to the configuration request for camera apps from VSM. The response received by server is 502 Bad Gateway.

Error:
Media server reported the error Device failed to configure Camera App Event

Workaround:
While configuring camera apps for 8000 series cameras, use camera firmware 1.0.9-9 and below.

7. Defect ID: CSCwe42496: In specific cases, Event edge recordings are groomed by camera from SD card.

Issue:
In specific cases, Event edge recordings are groomed by camera from SD card.

Event based SD card recording on 8k devices is not working. Camera detects the motion and generat es the event, but does not create the recording file as expected.

Affected Camera Models - 8020, 8000P, 8030 <<To confirm 8k series with Pratima>>

Tested Camera Firmware versions - 1.0.9-17, 1.0.9-12, 1.0.9-9, 1.0.7-4, 1.0.5-15, 1.0.3-4

Root cause:
Camera detects the motion and generates the event. In rare scenario the recording files are groomed by camera. This can be seen on the camera logs page of camera GUI. Camera logs suggesting event recording being purged with the log statement as shown below:

Mar 29 15:12:23 [STORMGR]: [Legacy_GenerateInsertSQL] **Remove a destroyed media**: /mnt/auto/CF/NCMF//20230329/15/event_motion20230329_151211.mp4, w (1920), h (1080), start_utc(1680082922), offset (19 over 0)

Also, sometimes Instead of creating the mp4 file of the recordings, the camera creates log file internally which results in no recordings available to VSM.

Workaround:
User can attempt below steps which might help overcome the issue:
1. Reboot camera
2. Format SD camera
3. Restore settings to Factory default

8. Defect ID: CSCwe70199: System reports Load Average Critical Alert on media server and Streaming Critical Alert for cameras.

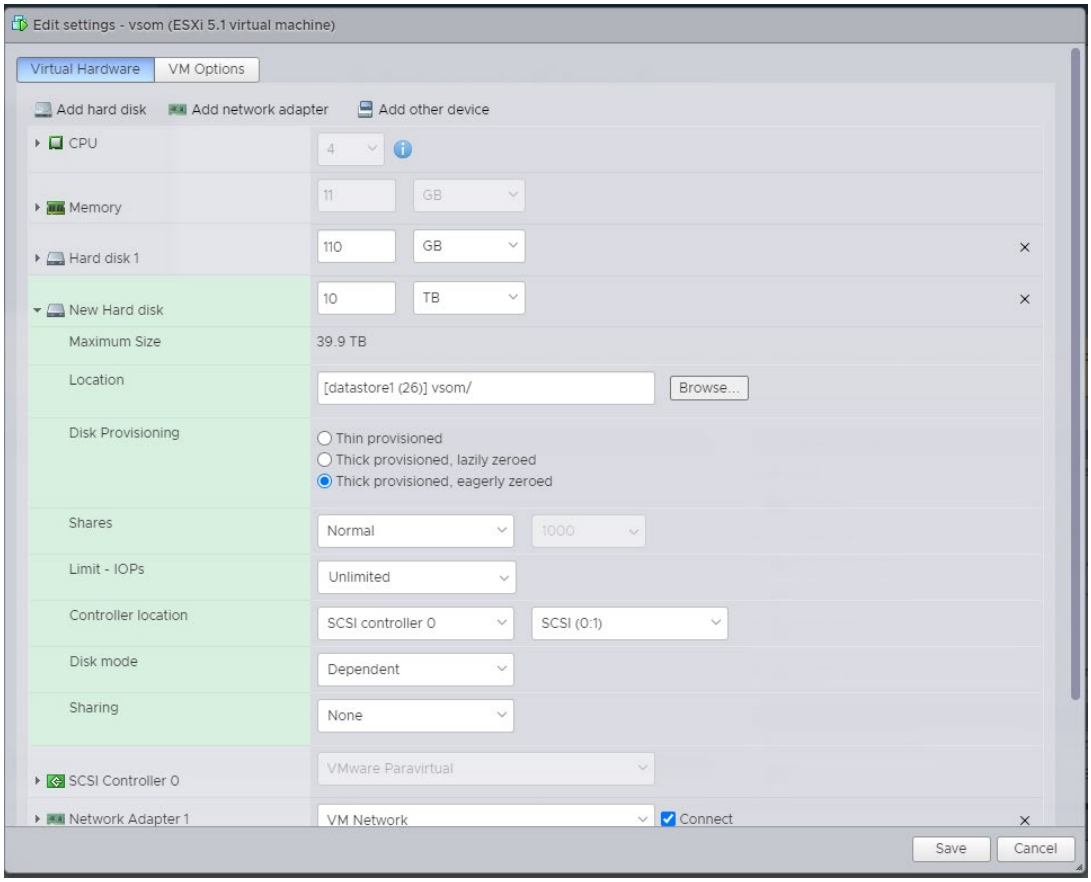
Issue:
System reports Load Average Critical Alert on media server and Streaming Critical Alert for cameras.

Issue could occur on Media server 7.14.7 deployed using OVA BC Edition on ESXi 6.7 (Underlying baremetal server M5 2RU). User can observe the “Queue overflow (Queue size-300)” errors in xvcrman.log file and then again can see the “Queue drained” messages in logs; Load average on the server can go very high and cameras generate alerts - “Streaming critical”.

Root cause:
Cause of such issues could be hardware/server specific. The issue was not reproducible on other machines. However, below workaround for any such issues could help to resolve.

Workaround:
To resolve the high load average issue on the non-working server - While adding the disk (media partitions) in new VM (deployed using VSM 7.14.7 BC OVA), select thick provisioning, eagerly zeroed option (This option will take time to create/add disk in VM as it zeroed/wipe out the all the data from drive) option (Tested with two drive/partition of size 10 TB each).

How to add the disk (all media partition) in VM -
1. Go to the respected VM by login in using ESXi or VCenter.
2. Select the “Edit” option in VM.
3. Now click on the “add hard disk” option (e.g., Add 10TB disk).
4. Follow the below snippet to config disk parameters -



5. Click on the “Save” option once disk configuration completes.

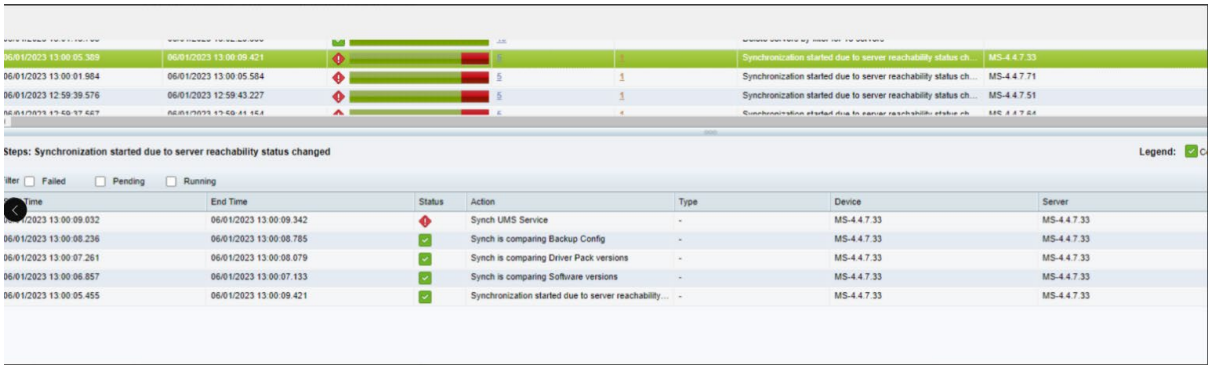
9. Defect ID: CSCwf58879: Server import job via csv is getting stopped.

Issue:
Server import job via csv is getting stopped.

While importing servers in bulk to VSOM, users may experience a situation where the user job appears to be completed, but upon checking the Jobs page, they observe that the import job has stopped at the end without finishing successfully.

Root cause:
Exact root cause of the issue is unknown. However, during lab tests, we could observe machines with higher RAM configurations could observe issue lesser. Issue could potentially be caused by a Java Heap Out of Memory (OOM) error as well.

Error:



Workaround:
Some options that can be tried to resolve this issue.
1. Try increasing RAM.
2. Increase the Java Heap memory on server. (Steps mentioned below)
3. If have virtual deployment then deploy the VSM-
7.14.7 OVA file with thick provisioned and eagerly zeroed option (While deployment only thick option avai lable and while adding new partition then thick provision, eagerly zeroed option available).

How to increase Java Heap Memory:

Note - Ensure server has sufficient RAM memory for application before increasing RAM for java heap space. Below steps increase the Java heap space to 4GB:

1. Open file /usr/BWhttpd/bin/init_tomcat
2. On lines 46 & 50 change JVM_MAX_MEMORY=?4096? (Default value is JVM_MAX_MEMORY="23 04")
3. On Line 53 change to "-Xms512m" (Default value is "-Xms256m")
4. Restart tomcat (/usr/BWhttpd/bin/init_tomcat restart)

10. Defect ID: CSCvz92063: Not able to login VSOM for some time due to the HttpServer coredumps on regular intervals.

Issue:
Not able to login VSOM for some time due to the HttpServer coredumps on regular intervals.

HttpServer core dump file is generated on regular intervals and while core file generation is in progress, user not able to login VSOM for some time.

Root cause:
Memory leak in Httpserver code causes OOM and creates coredump :

When Httpserver process's VIRT (virtual memory usage) reaches 4GB it results in OOM and crashes, this is a limit of 32-bit compiled libraries. So, whenever this process's usage goes near 4GB, any more malloc (memory allocation requests) results in a bad_alloc (allocation failures) thereby generating the abort/coredump with the same error. We can see libssl's "Out of Memory" logs and libstdc++ allocator failure in the dump, both the issues are result of ceiling limit reached by httpserver's VIRT usage.

This can be verified by pidstat -l -r| grep -i "httpserver" as below:

[root@M5-1ru-150 localadmin]# pidstat -l -r| grep -i httpserver
10:32:00 PM 0 5558 0.00 0.00 42440 6356 0.04 HttpServerMonitor . HttpServer
10:32:00 PM 0 5560 19.85 0.00 ***842616*** *695300 4.38* ***HttpServer***

Above **842616** is the VIRT value in KB, after five to seven days with heavily loaded server (Issue observed with 1400 cameras out of 450 not reachable), this value reaches near to 4GB eventually:

03:16:11 PM 0 11423 52.57 0.00 ***4193268*** *3563984 10.23* ***HttpServer***

Workaround:
Workaround: Monitor the HttpServer process memory utilization and restart the HttpServer process when reached the limit (3.8GB).

To access the patch details please search the defect ID in Bug Search Tool.

11. Defect ID: CSCwa10549: VMware Tools not available after upgrading to 7.14.X from 7.12.X and earlier.

Issue:
VMware Tools not available after upgrading to 7.14.X from 7.12.X and earlier.

Root cause:
VM tools tar file already available on VSM 7.12.X and earlier (RHEL 6) not working for VSM 7.14.X (For OS RHEL7 and RHEL8).

To check VM tools available on server or not execute below command:

systemctl status vmware-tools
Error: "Unit vmware tools service not found".

Or

systemctl status vmtoolsd
Error: " Unit vmtoolsd.service could not be found".

Workaround:
In RHEL7 and RHEL8 itself provided the VM tools through open-vm-tools package which need to install on the upgraded setup 7.14.X from 7.12.X and earlier.
To access the patch details, please search the defect ID in Bug Search Tool.

12. Defect ID: CSCwf82805: VSM 7.14.7: Load Average Critical Alert on Media Server Performance Setup

Issue:

VSM 7.14.7: Load Average Critical Alert on Media Server Performance Setup

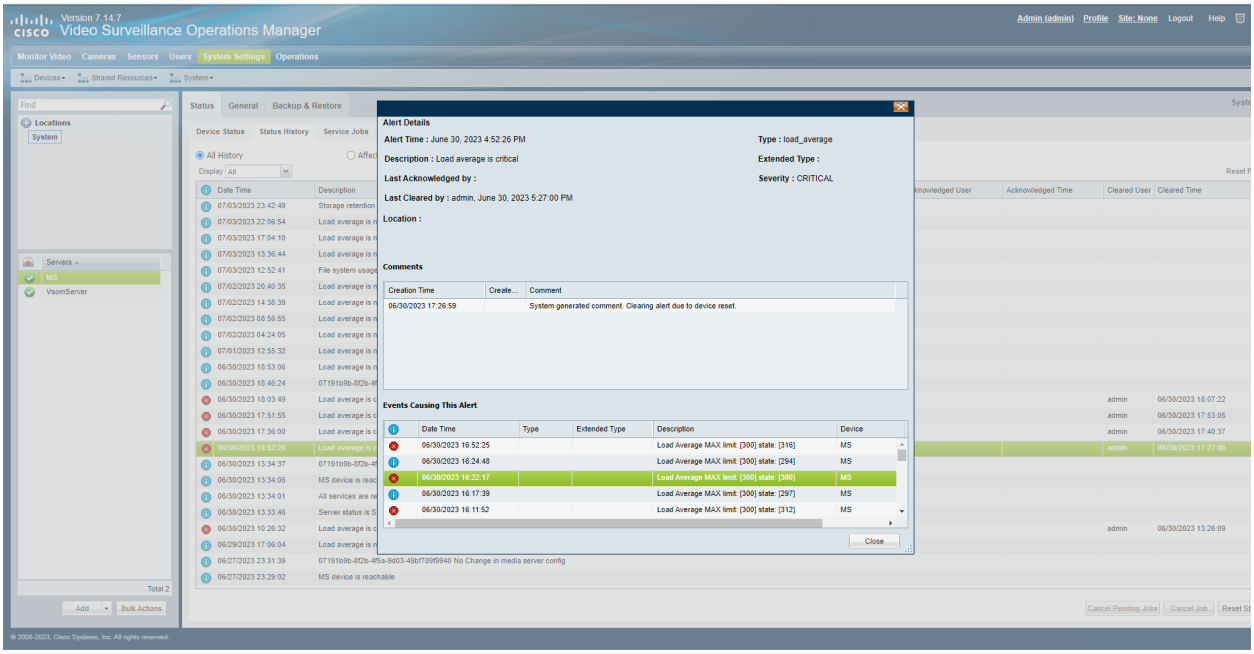
Root cause:

This load average critical alert due to the OS upgrade from RHEL 7 to RHEL 8, which user can ignore.

Load average alerts were created by VSM server if the 15 min load average crossed value of 12. To which scale value is 300, considering 4 cores on a VM and 11GB RAM (Same default configuration as BC edition OVA file.)

Apart from this load average critical alert, not observed any other alert or error on this server, IO wait on the disk also low which is around 12% to 15%.

Error: "Load average is critical"



Workaround:

If you do not want to see stale load average critical alerts, then scale up the 15 min load average value from 12 to 18, to which scale value is 450.

How to apply above changes on affected server -

1. SSH to the affected server.

2. Open the first file using command - vim /usr/BWhttpd/bin/installHMconfigs

3. Update the line number 18 -

From

LoadAverage <MAX> 300 </MAX>

To

LoadAverage <MAX> 450 </MAX>

4. Save the file.

5. Open the second file using command - vim /usr/BWhttpd/conf/serverHealth.cfg

6. Update the line number 5 -

From

LoadAverage <MAX> 300 </MAX>

To

LoadAverage <MAX> 450 </MAX>

7. Save the file.

8. Restart the systemmonitor process using command - /usr/BWhttpd/bin/init_sysmonitoring restart

Other Minor Issues on 7.14.7

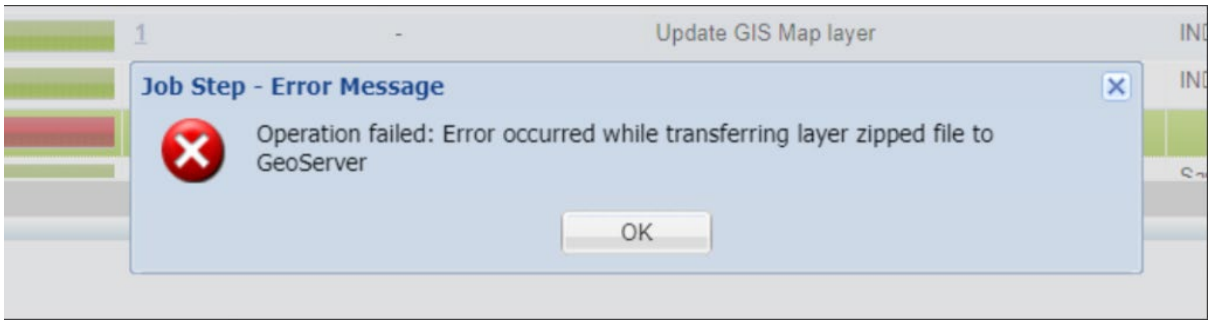
1. Issue while updating image layers from VSOM.

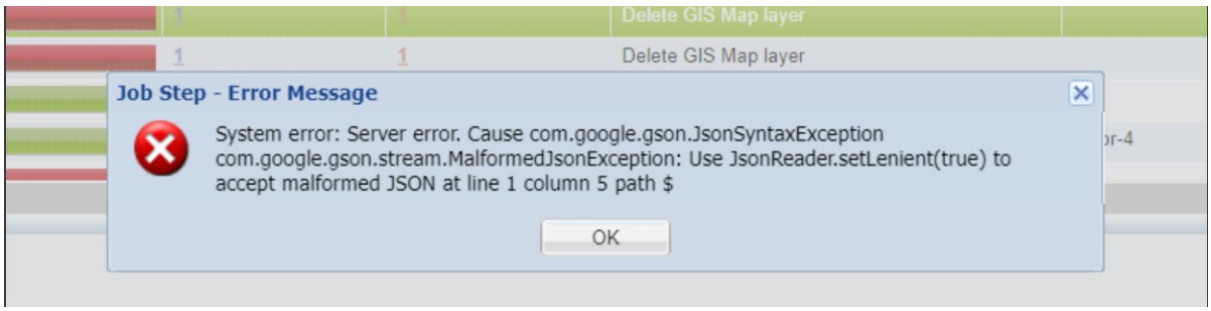
Issue:
While user tries to add/delete Image layers, the job fails with below mentioned error.

Root cause:
This is an intermittent issue. The intention to document this is only for user's knowledge.

Error:

Error occurred while transferring layer zipped file to GeoServer.





Workaround:
This was observed to be an intermittent issue. The job completes successfully on another attempt.

2. Issue during enabling VSOM service after fresh installation of 7.14.7 using OVA.

Issue:
System reports '*Application Initialization failed*' error when server is deployed using OVA.

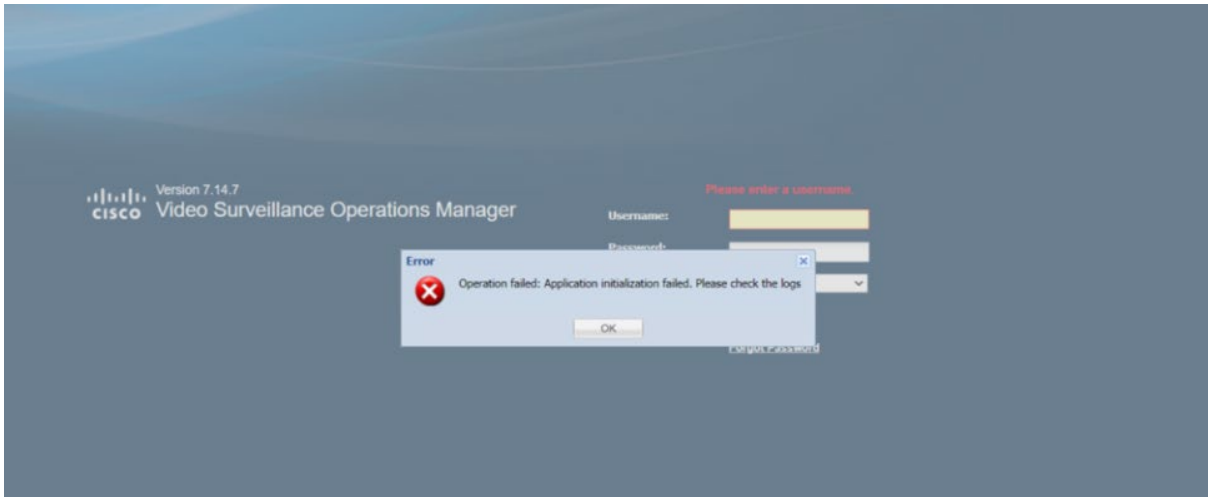
Error could be reported if user has assigned server VSOM role (standalone or co-located) after the installation.

Root Cause:

This is an intermittent issue caused by timeouts during the initialization process. User can instead use below workaround to overcome the issue.

Error:

Application initialization failed



Workaround:

On affected server run command - *sudo su service cisco restart*

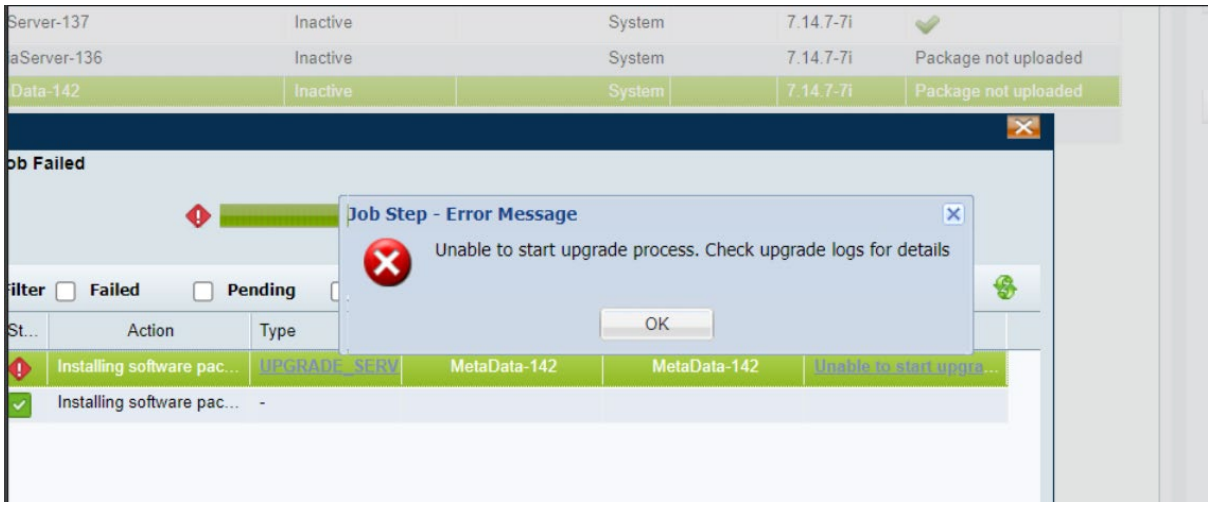
Troubleshooting Guide for Upgrade and Recovery

1. Issue:
An initial sub-job fails during the upgrade process from versions 7.14.5 and 7.14.6 to 7.14.7.

System throws shown error for an initial sub-job during the upgrade process. However, despite the sub-job failing, the system is still able to proceed and successfully complete upgradation.

Defect ID: CSCwd59320

Error:
Unable to start upgrade process

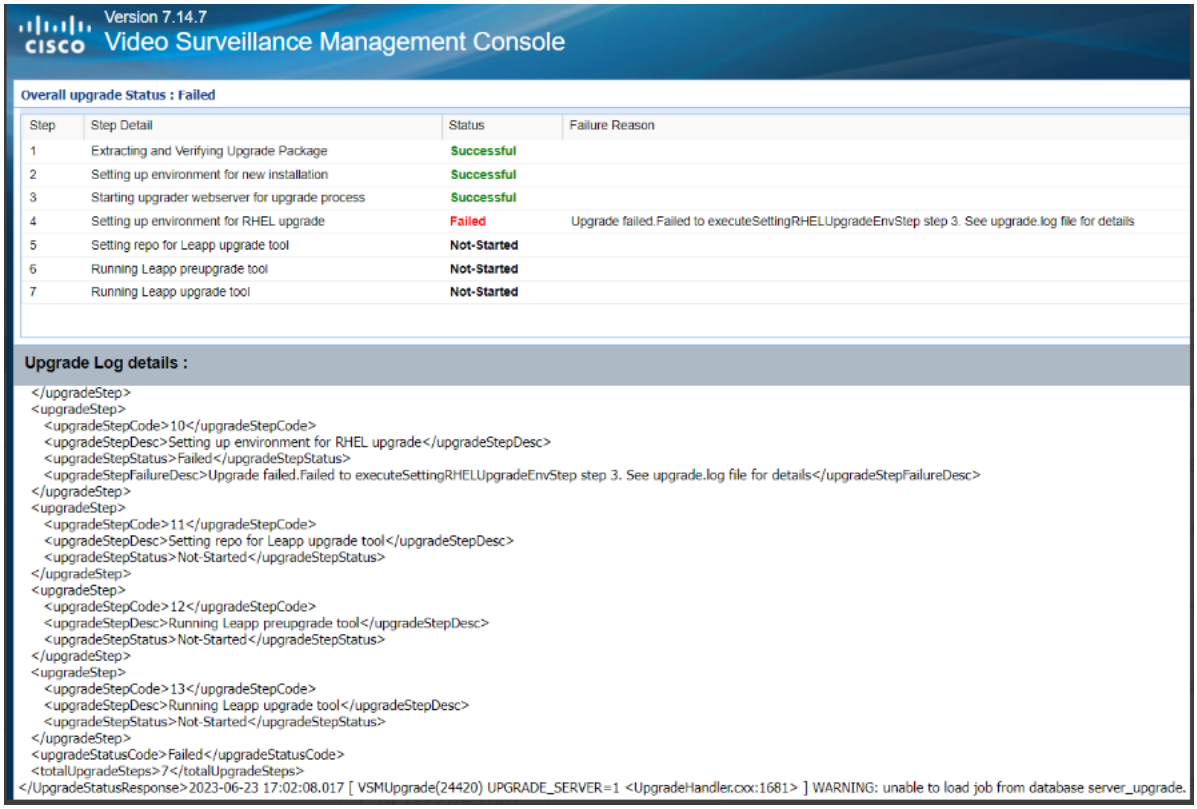


Steps to recover:

No workaround needed. The shown error has no impact on upgrade and system continues to upgrade successfully.

2. Issue:
Upgrade failed in executeSettingRHELUpgradeEnvStep

Error:



Steps to recover:

1. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,

   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

   warning: /etc/issue saved as /etc/issue.rpmsave

2. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpms from Cisco software download
   URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
3. Install redhat-release-server-7.6-4.el7.x86_64.rpm

   [root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_vsm_7.14.7_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

   warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

   Preparing... ## [100%]

   Updating / installing...

   1:redhat-release-server-7.6-4.el7 ## [100%]

4. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0

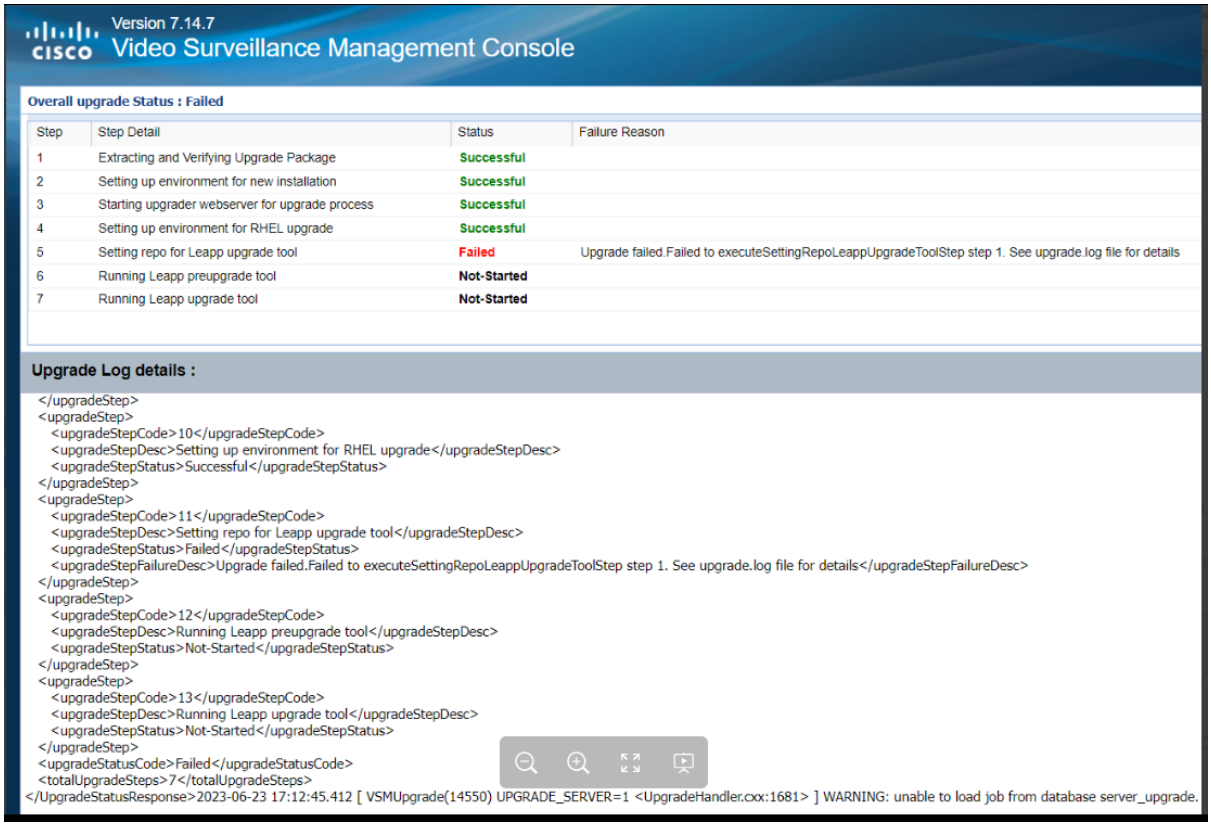
5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
6. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
7. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
8. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
9. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
10. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
11. [root@vsom-223 7.14.7-22i]# cat /etc/issue

    Red Hat Enterprise Linux Server release 7.6 (Maipo)

12. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
13. pkill VSMUpgrade
14. Trigger upgrade again from UI

3. Issue:
Upgrade failed in executeSettingRepoLeappUpgradeToolStep

Error:



Steps to recover:

1. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,

   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

warning: /etc/issue saved as /etc/issue.rpmsave

2. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpms from Cisco software download
   URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
3. Install redhat-release-server-7.6-4.el7.x86_64.rpm

   [root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

   warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

   Preparing... ################################# [100%]

   Updating / installing...

   1:redhat-release-server-7.6-4.el7 ################################# [100%]

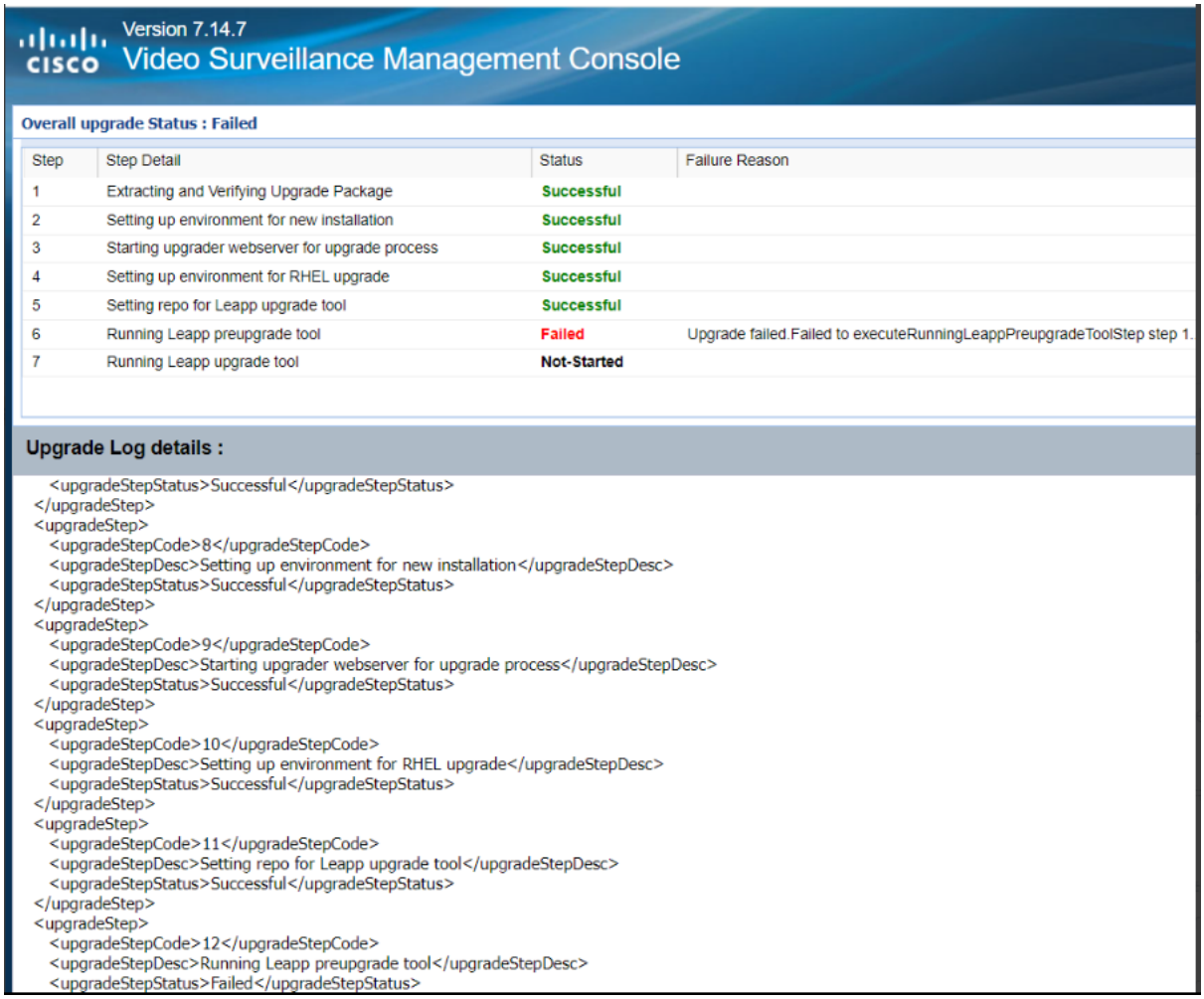
4. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0
5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
6. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
7. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
8. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
9. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
10. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
11. [root@vsom-223 7.14.7-22i]# cat /etc/issue

    Red Hat Enterprise Linux Server release 7.6 (Maipo)

12. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
13. pkill VSMUpgrade
14. Trigger upgrade again from UI

4. Issue:
Upgrade failed in executeRunningLeappPreupgradeToolStep

Error:



Steps to recover:

1. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,

   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

   warning: /etc/issue saved as /etc/issue.rpmsave

2. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpms from Cisco software download
   URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
3. Install redhat-release-server-7.6-4.el7.x86_64.rpm

   [root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_vsm_7.14.7_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

   warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

   Preparing... ## [100%]

   Updating / installing...

   1:redhat-release-server-7.6-4.el7 ## [100%]

4. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0
5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
6. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
7. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
8. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
9. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
10. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
11. [root@vsom-223 7.14.7-22i]# cat /etc/issue

    Red Hat Enterprise Linux Server release 7.6 (Maipo)

12. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
13. pkill VSMUpgrade
14. **Add rpm database entry for Cisco_VSBase rpm depending upon VSM version(VSM-7.14.5/VSM-7.14.6) from which you are upgrading,**
    a. **VSM-7.14.5 :** ***rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.5-015d-rhel5.8.rpm --nodeps***
    b. ***VSM-7.14.6 : rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.6-013d-rhel5.8.rpm --nodeps***
15. Trigger upgrade again from UI

5. Issue:
Upgrade to 7.14.7 failed from 7.14.5- Leapp download connection timeout for python3-firewall package.

Defect ID:
CSCwd97258

Error:

```
[MIRROR] python3-firewall-0.8.2-6.el8.noarch.rpm: Curl error (28): Timeout was reached for http://localhost:8080/RHEL8_Upgrade/BaseOS/Packages/python3-firewall-0.
8.2-6.el8.noarch.rpm [Operation too slow. Less than 1000 bytes/sec transferred the last 30 seconds]
[FAILED] python3-firewall-0.8.2-6.el8.noarch.rpm: No more mirrors to try - All mirrors were already tried without success

The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'dnf clean packages'.

STDERR:
Failed to create directory /var/lib/leapp/el8userspace//sys/fs/selinux: Read-only file system
Failed to create directory /var/lib/leapp/el8userspace//sys/fs/selinux: Read-only file system
No matches found for the following disable plugin patterns: subscription-manager
Error: Error downloading packages:
  Cannot download Packages/python3-firewall-0.8.2-6.el8.noarch.rpm: All mirrors were tried


============================================================
                      END OF ERRORS
============================================================


Debug output written to /var/log/leapp/leapp-upgrade.log

============================================================
                           REPORT
============================================================

A report has been generated at /var/log/leapp/leapp-report.json
A report has been generated at /var/log/leapp/leapp-report.txt

============================================================
                      END OF REPORT
============================================================

Answerfile has been generated at /var/log/leapp/answerfile


Dumping Upgrade Status Xml -

<?xml version="1.0" encoding="UTF-8"?>
```

```
Dumping Upgrade Status Xml -

<?xml version="1.0" encoding="UTF-8"?>
<UpgradeStatusResponse>
   <upgradeStep>
      <upgradeStepCode>0</upgradeStepCode>
      <upgradeStepDesc>Extracting and Verifying Upgrade Package</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>8</upgradeStepCode>
      <upgradeStepDesc>Setting up environment for new installation</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>9</upgradeStepCode>
      <upgradeStepDesc>Starting upgrader webserver for upgrade process</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>10</upgradeStepCode>
      <upgradeStepDesc>Setting up environment for RHEL upgrade</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>11</upgradeStepCode>
      <upgradeStepDesc>Setting repo for Leapp upgrade tool</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>12</upgradeStepCode>
      <upgradeStepDesc>Running Leapp preupgrade tool</upgradeStepDesc>
      <upgradeStepStatus>Successful</upgradeStepStatus>
   </upgradeStep>
   <upgradeStep>
      <upgradeStepCode>13</upgradeStepCode>
      <upgradeStepDesc>Running Leapp upgrade tool</upgradeStepDesc>
      <upgradeStepStatus>Failed</upgradeStepStatus>
      <upgradeStepFailureDesc>Upgrade failed.Failed to executeRunningLeappUpgradeToolStep step 1. See upgrade.log file for details</upgradeStepFailureDesc>
```

Steps to recover:

1. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,

   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

   warning: /etc/issue saved as /etc/issue.rpmsave

2. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpms from Cisco software download
   URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
3. Install redhat-release-server-7.6-4.el7.x86_64.rpm

[root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_vsm_7.14.7_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

Preparing... ################################# [100%]

Updating / installing...

1:redhat-release-server-7.6-4.el7 ################################# [100%]

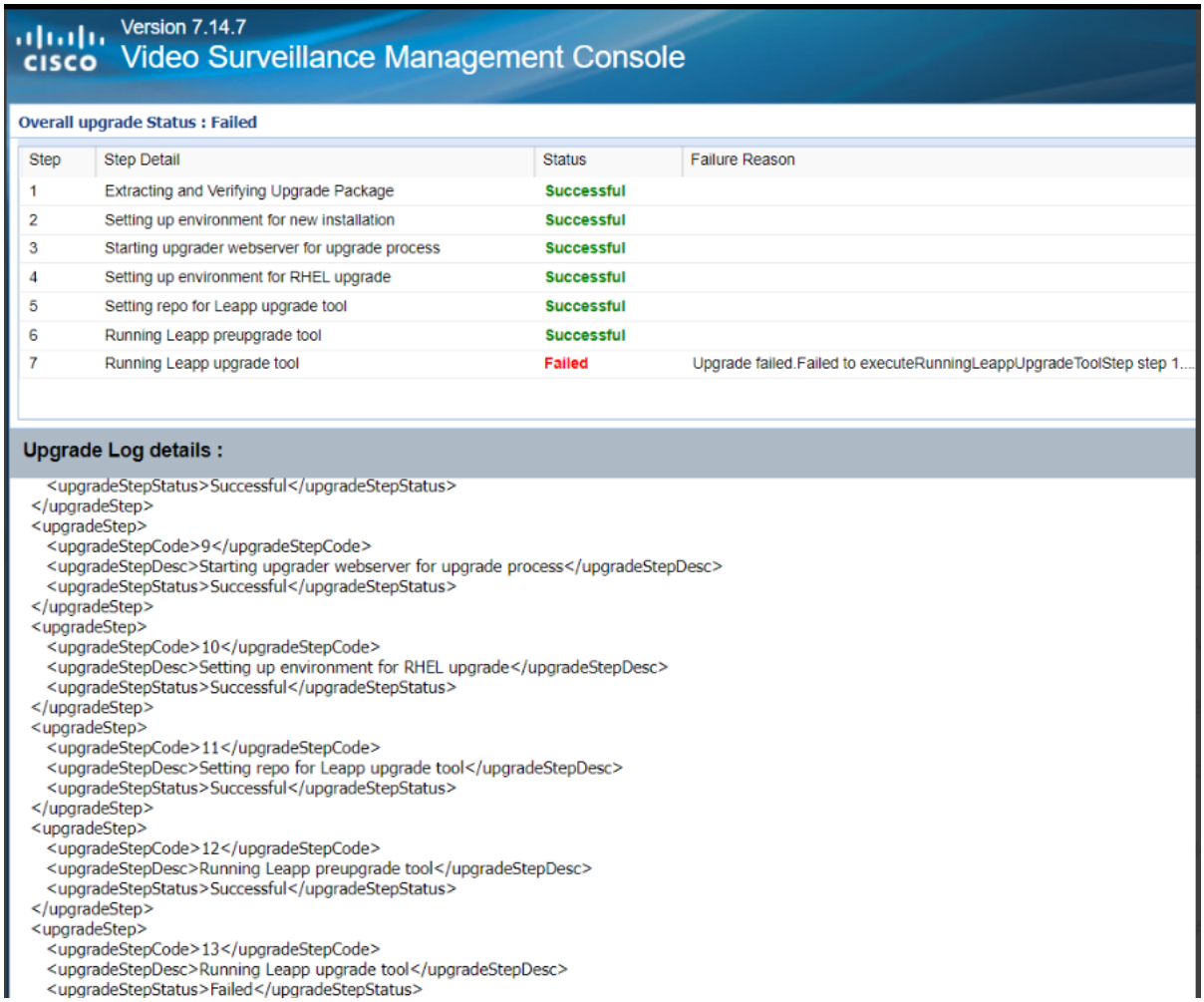
4. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0
5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
6. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
7. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
8. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
9. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
10. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
11. [root@vsom-223 7.14.7-22i]# cat /etc/issue

    Red Hat Enterprise Linux Server release 7.6 (Maipo)

12. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
13. pkill VSMUpgrade
14. **Add rpm database entry for Cisco_VSBase rpm depending upon VSM version(VSM-7.14.5/VSM-7.14.6) from which you are upgrading,**
    a. **VSM-7.14.5 :** ***rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.5-015d-rhel5.8.rpm --nodeps***
    b. ***VSM-7.14.6 : rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.6-013d-rhel5.8.rpm --nodeps***
15. Trigger upgrade again from UI

6. Issue:
Upgrade failed in executeRunningLeappUpgradeToolStep

Error:



Steps to recover:

1. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,

   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

   warning: /etc/issue saved as /etc/issue.rpmsave

2. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpms from Cisco software download
   URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
3. Install redhat-release-server-7.6-4.el7.x86_64.rpm

   [root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_vsm_7.14.7_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

   warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

   Preparing... ## [100%]

   Updating / installing...

1:redhat-release-server-7.6-4.el7 ################################# [100%]

4. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0
5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
6. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
7. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
8. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
9. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
10. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
11. [root@vsom-223 7.14.7-22i]# cat /etc/issue

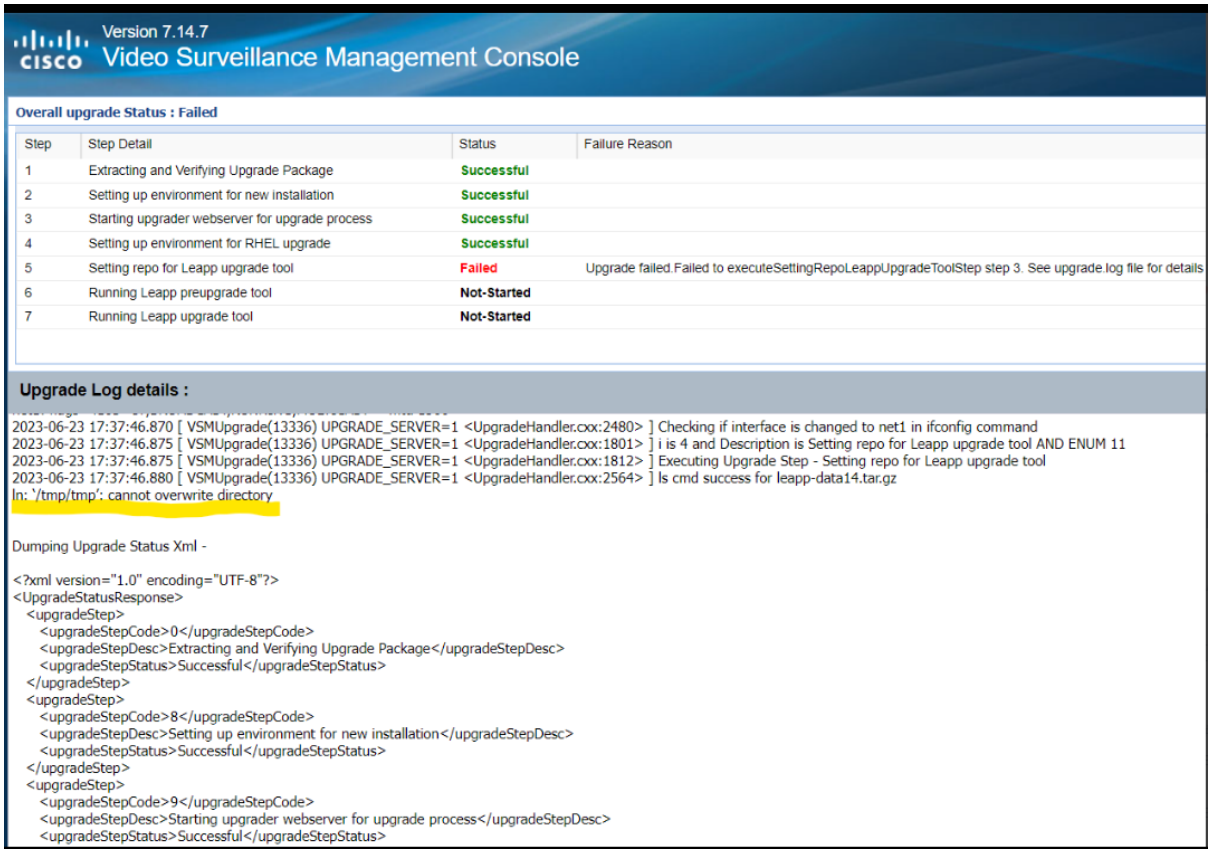
    Red Hat Enterprise Linux Server release 7.6 (Maipo)

12. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
13. pkill VSMUpgrade
14. **Add rpm database entry for Cisco_VSBase rpm depending upon VSM version(VSM-7.14.5/VSM-7.14.6) from which you are upgrading,**
    a. **VSM-7.14.5 :** ***rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.5-015d-rhel5.8.rpm --nodeps***
    b. ***VSM-7.14.6 : rpm -Uvh --force --justdb /<path_vsm_7.14.7_opt_rpms_copied>/Cisco_VSBase-7.14.6-013d-rhel5.8.rpm --nodeps***
15. Trigger upgrade again from UI

7. Issue:
Media server upgrade failed with ‘failed to create symbolic link ‘/tmp/tmp’: File exists’ error.

Defect ID:
CSCwd60618

Error:



Steps to recover:

1. **Remove tmp folder from /tmp with this command,** ***rm -rf /tmp/tmp***
2. Remove redhat-release-server-7.9-6.el7_9 rpm with below command,
   rpm -e --noscripts --nodeps redhat-release-server-7.9-6.el7_9.x86_64,

   warning: /etc/issue saved as /etc/issue.rpmsave

3. Download <Cisco_VSM_7.14.7_opt_rpms_CSCwd60618_CSCwd97258.zip> the required rpm(redhat-release-server-7.6-4.el7.x86_64.rpm) from Cisco software download URL: https://software.cisco.com/download/home/282976740/type/281933881/release/7.14.7
4. Install redhat-release-server-7.6-4.el7.x86_64.rpm

   [root@vsom-223 7.14.7-22i]# rpm -Uvh /<path_vsm_7.14.7_opt_rpms_copied>/redhat-release-server-7.6-4.el7.x86_64.rpm

   warning: /root/redhat-release-server-7.6-4.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY

   Preparing... ## [100%]

   Updating / installing...

   1:redhat-release-server-7.6-4.el7 ## [100%]

5. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net0 /etc/sysconfig/network-scripts/ifcfg-eth0

6. [root@vsom-223 7.14.7-22i]# mv /etc/sysconfig/network-scripts/ifcfg-net1 /etc/sysconfig/network-scripts/ifcfg-eth1
7. Replace net0 with eth0 in /etc/sysconfig/network-scripts/ifcfg-eth0
8. Replace net1 with eth1 in /etc/sysconfig/network-scripts/ifcfg-eth1
9. [root@vsom-223 7.14.7-22i]# ip link set net0 down && ip link set net0 name eth0 && ip link set eth0 up
10. [root@vsom-223 7.14.7-22i]# ip link set net1 down && ip link set net1 name eth1 && ip link set eth1 up
11. [root@vsom-223 7.14.7-22i]# cat /etc/redhat-release > /etc/issue
12. [root@vsom-223 7.14.7-22i]# cat /etc/issue

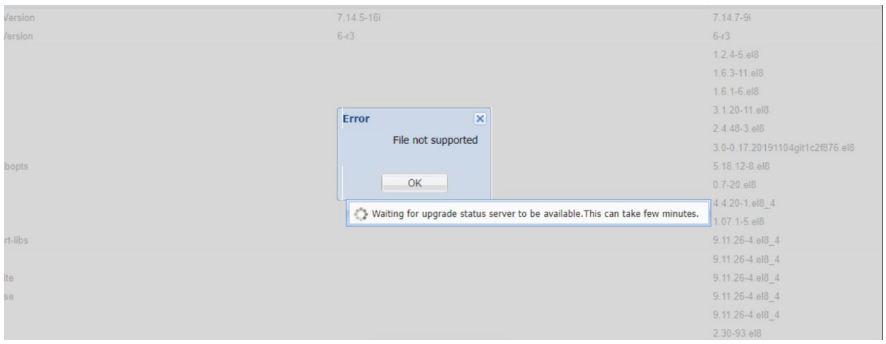
    Red Hat Enterprise Linux Server release 7.6 (Maipo)

13. rm -rf /var/reboot_rhel_upgrade_7_to_8_network_name_change
14. pkill VSMUpgrade
15. Trigger upgrade again from UI

8. Issue:
Redundant Pop-up Alert showing up - File not supported, while upgrading to 7.14.7 from CDAF server. This is an internal error caused due to an unsupported file type is in VSM software.

Defect ID: CSCwd82293

Error:
File not supported.

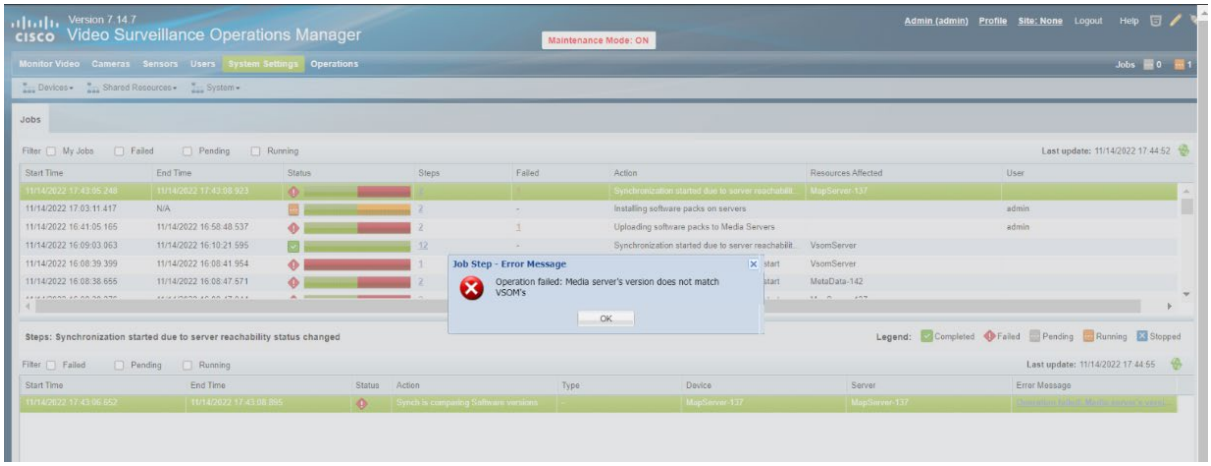


Steps to recover:
No workaround needed. This error is just dialog box. Irrespective of user intervention upgrade process runs smoothly and successfully.

9. Issue:
Redundant Synchronization job internal to upgrade process are failing during upgrade.

Defect ID: CSCwd61839

Error:



Steps to recover:

No workaround is needed. These job failures can be ignored since they don’t impact upgrade.

Appendix

Upgrade instructions for VSM with SAN storage

Upgrading VSM to version 7.14.0 or higher, may run into issue with SAN setup running as RAW Disk on VM's. This is a Known issue acknowledged by RedHat; A solution is provided by RedHat which suggests setting SCSI parameter for a VM setting to "True" in order to upgrade Red-Hat OS and VSM version

Red Hat article reference- https://access.redhat.com/solutions/3661051

We advise to apply the below solution before you upgrade to 7.14.0 and higher versions.

If you missed the step before upgrade, and if you see the same symptoms then you can still apply the step after the upgrade and restart the server.

There are two ways to edit SAN parameters for VM settings.

1. Auto - tool/script that updates the parameter for all VMs for and ESXiserver, Contact Cisco Technical Assistance Centre.

2. Manual - Steps as below.

- Run the following command on the each server to find out scsi controller and target number for each drives.

  ```
  # cat /proc/scsi/scsi
  ```

  Example output :
  Host: scsi1 Channel: 00 Id: 02 Lun: 00
  Vendor: XYZ Storage Model: ABC Rev: 1.0
  Type: Direct-Access ANSI SCSI revision: 05

  Note scsi# and ID# for each drive.
- Power off Virtual machines.

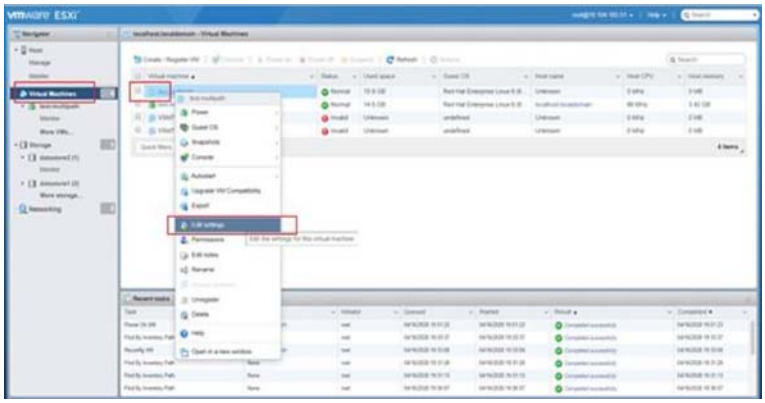
- Edit .vmx file of each Media Server Virtual Machine. Perform below steps from ESXi server to configure .vmx file
  a. Connect to the ESXi server
  b. Click Edit Settings, then select “VM Options”.
  c. Scroll down to “Configuration Parameters” and click “Edit Configuration”.
  d. Click “Add parameter”.
  e. For each LUN add ‘ignoreDeviceInquiryCache’ as below

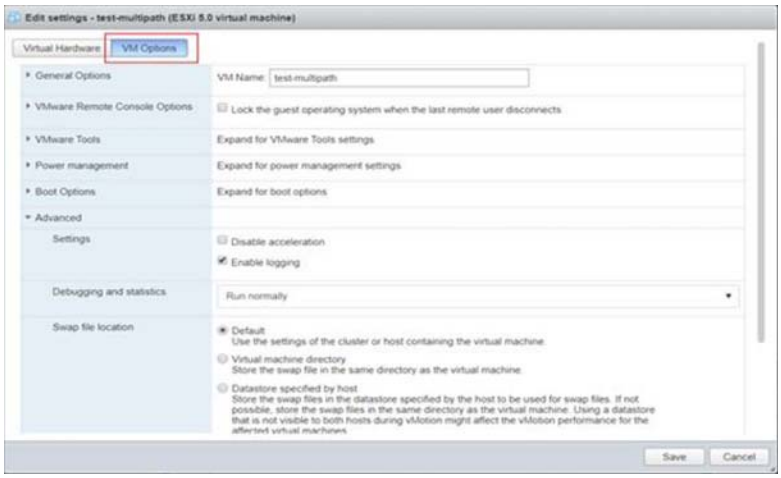
```
Key = scsiX:Y.ignoreDeviceInquiryCache
Value = true
```

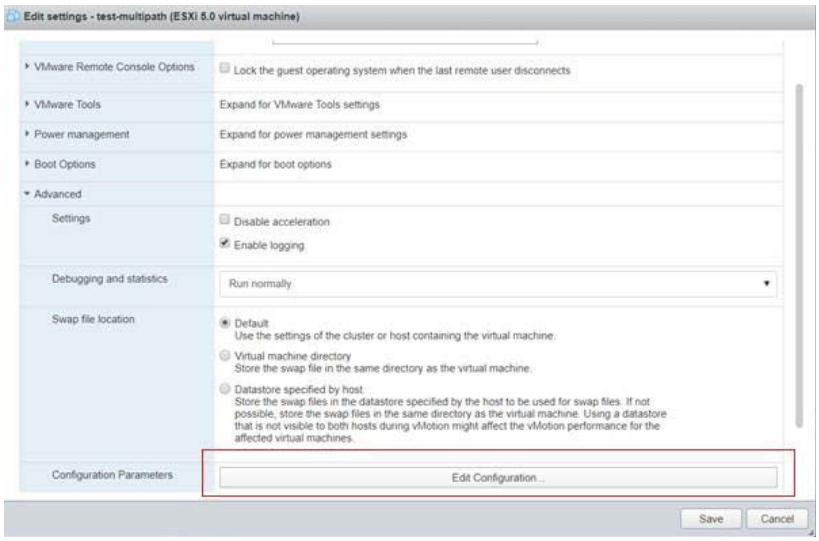
where X,Y are SCSI controller number and SCSI target number noted in step 1.

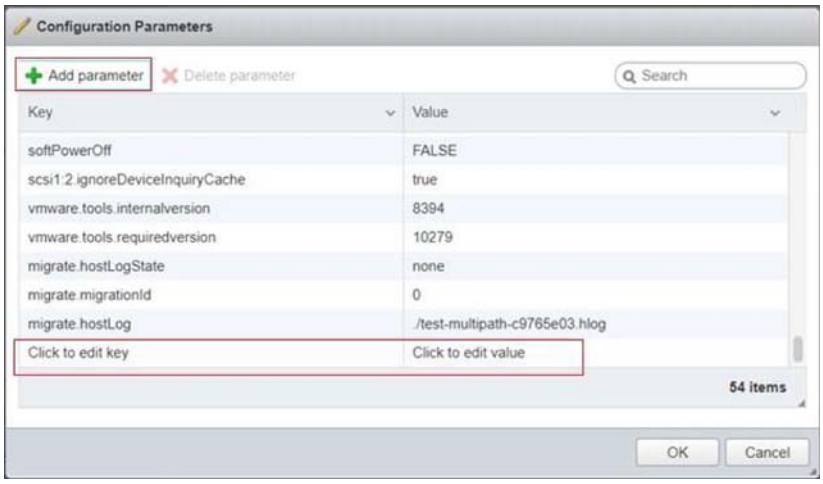
Click OK and Save settings.

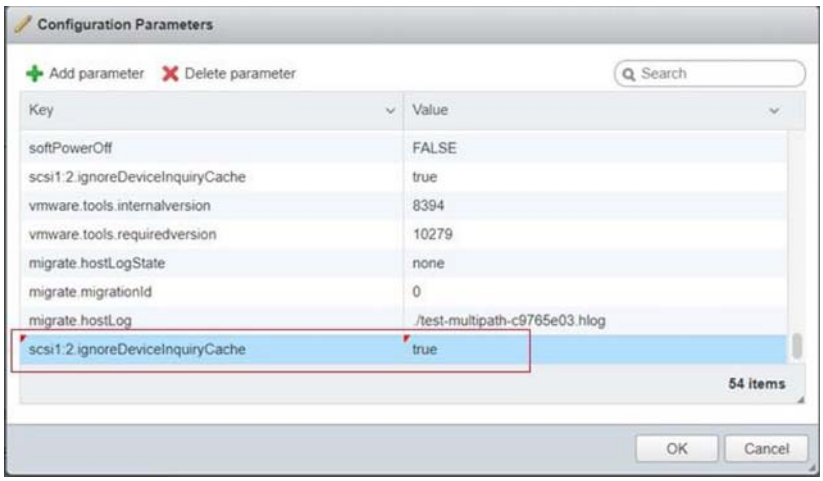
Below are the images for reference






Edit settings - test-multipath (ESXi 5.0 virtual machine)
VMware Remote Console Options
Lock the guest operating system when the last remote user disconnects
VMware Tools
Expand for VMware Tools settings
Power management
Expand for power management settings
Boot Options
Expand for boot options
Advanced
Settings
Disable acceleration
Enable logging
Debugging and statistics
Run normally
Swap file location
Default
Use the settings of the cluster or host containing the virtual machine.
Virtual machine directory
Store the swap file in the same directory as the virtual machine.
Datastore specified by host
Store the swap files in the datastore specified by the host to be used for swap files. If not possible, store the swap files in the same directory as the virtual machine. Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines.
Configuration Parameters
Edit Configuration...
Save
Cancel


Configuration Parameters
Add parameter
Delete parameter
Search
Key
Value
softPowerOff
FALSE
scsi1:2.ignoreDeviceInquiryCache
true
vmware.tools.internalversion
8394
vmware.tools.requiredversion
10279
migrate.hostLogState
none
migrate.migrationId
0
migrate.hostLog
./test-multipath-c9765e03.hlog
Click to edit key
Click to edit value
54 items
OK
Cancel


Configuration Parameters
Add parameter
Delete parameter
Search
Key
Value
softPowerOff
FALSE
scsi1:2.ignoreDeviceInquiryCache
true
vmware.tools.internalversion
8394
vmware.tools.requiredversion
10279
migrate.hostLogState
none
migrate.migrationId
0
migrate.hostLog
./test-multipath-c9765e03.hlog
scsi1:2.ignoreDeviceInquiryCache
true
54 items
OK
Cancel

- Power on servers.
- Follow regular upgrade process.

Related Documentation

See the following locations for the most current information and documentation:

Cisco Video Surveillance 7 Documentation Roadmap

Descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

http://www.cisco.com/go/physicalsecurity/vsm/roadmap

Cisco Physical Security Product Information:

www.cisco.com/go/physicalsecurity/

Cisco Video Surveillance Manager Documentation Website

www.cisco.com/go/physicalsecurity/vsm/docs

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Release Notes for Cisco Video Surveillance Manager, Release 7.14.7
© 2008 - 2023 Cisco Systems, Inc. All rights reserved.