Cisco Video Surveillance Manager: Install and Upgrade Guide, Release 7.6

Release 7.6

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Video Surveillance Manager: Install and Upgrade Guide, Release 7.6

Preface

Revised: October 21, 2015

This document, the *Cisco Video Surveillance Manager: Install and Upgrade Guide* provides instructions to install and upgrade the various software components used in a Cisco Video Surveillance Manager (Cisco VSM) deployment. See the "Overview" section on page 1 for more information about the different type of software used in a deployment.

Note This guide does not describe how to install the hardware (such as servers, cameras, or other devices) that are also used in a Cisco VSM deployment. See the hardware documentation for more information.

Related Documentation

See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists all new and revised Cisco technical documentation. It is available at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Tip See Related Documentation for more information and links to Cisco Video Surveillance documentation.

Overview

A Cisco Video Surveillance Manager (Cisco VSM) deployment includes Cisco VSM servers (such as Media Server, Operations Manager server, Maps server, etc), and the software that runs on the cameras, encoders, and client PCs in your deployment.

Installing or upgrading Cisco VSM entails installing or upgrading the Cisco VSM server system software, device driver packs, device firmware, and client workstations. When upgrading, these tasks should be performed in a specific order, and must be completed on all devices, servers, and PCs in your deployment.

This chapter includes the following information:

Installation and Upgrade Summary

Deploying a new system is similar to upgrading an existing system: the system (server) software, device driver packs, device firmware, and client monitoring software must all be upgraded to the version supported by your Cisco VSM release.

The main difference between a new system and an existing system is that the system software and driver packs are pre-installed on new physical servers. Upgrades require that these software components also be upgraded.

Refer to the following topics for summaries of the main installation and upgrade tasks:

- Deploying a New System, page 1-2
- Upgrading an Existing System, page 1-3

Deploying a New System

Complete the following basic tasks to deploy a l Cisco Video Surveillance Manager (Cisco VSM) system:

Summary Steps

Table 1-1 Deploy a New System: Summary Steps

	Upgrade Task	Description	Complete?
Step 1	System Software	Install the Cisco VSM server or virtual machine (VM): • Purchase and install the physical Cisco Connected Safety and Security UCS series server as described in the Cisco Physical Security UCS Platform Series User Guide. These servers are pre-installed with the latest Cisco VSM system software and device driver packs. • Deploy one or more Cisco VSM virtual machines (VMs) on a Cisco Connected Safety and Security UCS series server. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.	❑
Step 2	Server setup	Complete the Initial Setup Wizard, page 2-2 to perform the one-time Cisco VSM setup.	❑
Step 3	Driver Packs	Update the server driver packs, if necessary, to support the cameras and encoders that will be added to the system. See Installing and Upgrading Driver Packs, page 4-1.	❑
Step 4	Firmware	Update the firmware on the cameras and encoders that will be added to the system. See Upgrading Cisco Camera and Encoder Firmware, page 5-1.	❑
Step 5	Cisco SASD (desktop software)	Install the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) monitoring software on your client PCs. • You can install Cisco SASD before or after the Operations Manager server is installed. The server and Cisco SASD version must be the same, or the PC application will not launch. • See Installing Cisco Video Surveillance Safety and Security Desktop (Cisco SASD), page 6-1.	❑

Table 1-1 Deploy a New System: Summary Steps (continued)

	Upgrade Task	Description	Complete?
Step 6	Multipane client software	On each monitoring PC, follow the prompts to upgrade the Cisco Multi-Pane client software when you first log in to Cisco SASD or the Operations Manager. The Multi-Pane client is an Active X client that enables video playback and other features. Users cannot play video if the Multi-Pane client version is missing, or different than the Operations Manager server.	❑
Step 7	Feature config	Perform additional configuration and operation tasks as described in the Cisco Video Surveillance Operations Manager User Guide.	❑
Step 8	Language Packs	(Optional) Install language packages to display the Cisco Video Surveillance interface in additional languages, if necessary. See Upgrading Language Packs, page 7-1.	❑

Upgrading an Existing System

Upgrading a previously-installed Cisco VSM deployment entails similar tasks as a new system, but you must upgrade the servers in a specific order, and you do not need to complete the Initial Setup Wizard.

After the servers are upgraded, you must upgrade the cameras, encoders, and monitoring workstations (PCs) to the supported release.

Tip See the Release Notes for Cisco Video Surveillance Manager for information about the firmware and driver packs supported in your release. The Cisco SASD monitoring software on each PC must also match the system software release running on the Cisco Video Surveillance Manager.

Summary Steps

Table 1-2 Upgrade an Existing System: Summary Steps

	Software Upgrade	Task	Complete?
Step 1	System Software	Upgrade the system software on the Cisco VSM servers or virtual machines (VMs). • Use the Operations Manager user interface to upgrade physical and virtual machines. See Upgrading System Software, page 3-1. • Upgrade the servers in the order specified in Server Upgrade Sequence, page 3-4.	❑
Step 2	Driver Packs	Upgrade the server driver packs, if necessary, to support the cameras and encoders that will be added to the system. See Installing and Upgrading Driver Packs, page 4-1.	❑
Step 3	Firmware	Upgrade the firmware on the cameras and encoders in your deployment. • The device firmware is required to support new or revised features. See the Release Notes for Cisco Video Surveillance Manager for the device firmware required by your release. • See Upgrading Cisco Camera and Encoder Firmware, page 5-1.	❑

Table 1-2 Upgrade an Existing System: Summary Steps (continued)

	Software Upgrade	Task	Complete?
Step 4	Cisco SASD (desktop software)	Upgrade the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) monitoring software on your client PCs. You can update Cisco SASD before or after the Operations Manager server is upgraded, but the server and Cisco SASD version must be the same, or the PC application will not launch. See Installing Cisco Video Surveillance Safety and Security Desktop (Cisco SASD), page 6-1	❑
Step 5	Multipane client software	On each monitoring PC, follow the prompts to upgrade the Cisco Multi-Pane client software when you first log in to Cisco SASD or the Operations Manager. The Multi-Pane client is an Active X client that enables video playback and other features. Users cannot play video if the Multi-Pane client version is different than the Operations Manager server.	❑
Step 6	Feature config	Perform additional configuration and operation tasks as described in the Cisco Video Surveillance Operations Manager User Guide.	❑
Step 7	Language Packs	(Optional) Install language packages to display the Cisco Video Surveillance interface in additional languages, if necessary. See Upgrading Language Packs, page 7-1.	❑

Understanding Cisco Video Surveillance Software

The following table summarizes the software that can be upgraded in a Cisco VSM deployment.

Table 1-3 Cisco Video Surveillance Software Types

Software Type	Description
System software	*System Software* is the Cisco VSM server software that includes the Media Server, Operations Manager, Management Console, Maps Server and other server services. Use the Operations Manager to update the *System Software* on all servers (such as Media Servers) associated with the Operations Manager. **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 and use the **Server Upgrade** feature.
OVA image (for VM installations)	OVF template files are used to install the server 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-7.6.0-331d_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.
Device *firmware*	Device *firmware* is provided by the device manufacturer. The firmware for Cisco devices can be upgraded using Operations Manager (as described in the "Upgrading Cisco Camera and Encoder Firmware" section on page 5-1). Firmware for devices from non-Cisco manufacturers is upgraded using a direct connection to the device. Refer to the device documentation for more information.
Device *driver packs*	Device *driver packs* are the software packages used by Media Server and 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 (**System Settings > Driver Pack Management**). See the "Installing and Upgrading Driver Packs" section on page 4-1 for instructions. **Note** We strongly recommend upgrading driver packs using the Operations Manager interface. This allows you to upgrade multiple servers at once. Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled. The Management Console interface can also be used to upgrade the driver packs for a single server at a time. • *Driver pack* versions must be the same on the servers that host the Media Server and Operations Manager or a *driver pack mismatch* error. Templates cannot be revised when a *driver pack mismatch* error is present.

Table 1-3 Cisco Video Surveillance Software Types (continued)

Software Type	Description
Language Packs	Language packs can be added to display the VSM user interfaces in non-English languages. Language packs are added using the Operations Manager. See "Upgrading Language Packs" section on page 7-1.
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 Video Surveillance Manager Recovery Guide for your hardware platform for more information.

Tip For information about supported software releases, see the Release Notes for Cisco Video Surveillance Manager.

Understanding System Software

Cisco VSM system software is pre-installed on new servers. You can also install system software as a virtual machine, or upgrade an existing deployment using upgrade images downloaded from the cisco.com website.

Cisco VSM Installation and Upgrade Options

Cisco VSM is pre-installed in new servers, or can be upgraded on an existing Cisco VSM server, or installed as a virtual machine (VM):

Table 1-4 Cisco VSM Installation and Upgrade Options

Option	Description	Notes
Pre-installed	Cisco VSM is pre-installed in new installations on the Cisco Connected Safety and Security UCS Platform Series servers CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9.	See Deploying a Physical Cisco VSM Server, page 2-1 for more information.
Upgrade from Release 7.2.1 or higher	Cisco VSM Release 7.2.1 and higher can be upgraded directly to the latest release using a `.zip` upgrade file that includes all required software packages. • You can upgrade Cisco VSM virtual machines (VMs) or Cisco Video Surveillance servers. • Servers include the Cisco Multiservices Platform (Cisco MSP) and the Cisco Connected Safety and Security UCS Platform Series servers.	See Upgrading System Software, page 3-1 for more information. **Note** To upgrade from 7.2.0 or earlier, upgrade to r7.2.1 or 7.2.2 or 7.5 first, and then upgrade to the latest release.
Virtual Machine (OVA templates)	To create a new virtual machine (VM) instance of the server, install the Cisco VSM .OVA template file on a Cisco UCS server CPS-UCS-1RU-K9 or CPS-UCS-2RU-K9. **Note** 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.

Understanding Server Services

Server services are activated during the initial server setup, and managed using the browser-based Operations Manager.

After a server is added to the Operations Manager configuration, the Management Console cannot be used to activate or deactivate the server services. Use the Operations Manager to manage server services. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Usage Notes

- The Operations Manager must be enabled using the Management Console.
- The Federator or Metadata service can only be added as a standalone server using the Management Console if the server is unmanaged, or Operations Manager if the server is managed.
- If the Operations Manager is not co-located on the server, you can remove the server from Operations Manager management and then activate or deactivate any of the available services.

Supported Services

Cisco VSM servers can support the following server services. See the release notes for the services supported by your deployment.

Table 1-5 Supported Server Services

Service	Description	Activation Rules
Operations Manager	The browser-based Cisco VSM Operations Manager administration and configuration tool.	Can be added as a stand-alone server, or co-located with other services (such as a Media Server). The Maps server can also be co-located with the Operations Manager in Release 7.6 and higher. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. Select the **Operations Manager** service. 3. (Optional) Select the Media Server service to create a co-located server. This automatically enable the Media Server service on the default "VSOMServer". **Note** At least one Media Server must be added to the Operations Manager for the system to be functional. 4. Log in to the Operations Manager to further configure the services and system features. **To Disable:** 1. Log in to the Management Console for each server associated with the Operations Manager server and click the **Remove** button. **Note** The **Remove** button disassociates the server and all server services from the Operations Manager. This allows the server (and running services) to be added and managed by a different Operations Manager. 2. Log in to the Operations Manager server and deselect the **Operations Manager** service

Table 1-5 Supported Server Services (continued)

Service	Description	Activation Rules
Media Server	The Media Server service provides video streaming, recording and storage for the cameras and encoders associated with that server. Media Servers can also be configured for high availability, and provide Redundant, Failover, and Long Term Storage	Can be added as a stand-alone server, or co-located on a single server with the Operations Manager. Can also be co-located with the Maps Server in release 7.6 and higher. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. (Co-located server) Log in to the Operations Manager, select **System Settings > Server**, and select the default **VSOMServer**. In the Services section, select the **Media Server** service. 3. (Stand-alone server) Log in to the Operations Manager and add the server as a **Media Server**. 4. Select the Media Server **Advanced** settings to further configure the service, if necessary. **To Disable:** • Log in to the Operations Manager, select **System Settings > Server**, select the server, and deselect the **Media Server** service. or • Log in to the Management Console for the server, and click *Remove* to remove the server from the Operations Manager. Then de-select the service.
Map Server	Allows Image Layers to be added to location maps using the Operations Manager. Image layers are viewed by operators using the Cisco Video Surveillance Safety and Security Desktop application. Cameras, locations and alerts are displayed on dynamic maps, and map images that represent the real-world location of devices and events.	Install the Maps Server as standalone server or use the Operations Manager to activate the service as a co-located service). **Note** A stand-alone Maps server requires the RHEL 6.4 64 bit OS. **To Enable a Stand-Alone Server:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Maps Server**. 3. Configure the Location Maps using the Operations Manager. **To Enable a Co-Located Maps Server:** 1. Install the Operations Manager server. 2. Log in to the Operations Manager. 3. Navigate to the Operations Manager server configuration page. 4. Select the **Maps Server** service on the Operations Manager server. 5. Configure the Location Maps using the Operations Manager. **To Disable:** • If the Operations Manager is not co-located with the Maps Server, log in to the Management Console for the server, click **Remove** to remove the server from the Operations Manager, and then deselect the service. • If the Operations Manager is co-located with the Maps Server, log in to the Operations Manager and deselect the Media Server service.

Table 1-5 Supported Server Services (continued)

Service	Description	Activation Rules
Metadata Server	Allows metadata to be added to recorded video, which enables features such as Video Motion Search in the Cisco SASD desktop application. Metadata can also be accessed by 3rd party integrators for advanced analytics analysis.	Use the Operations Manager to activate the service. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Install the server and complete the Management Console Setup Wizard. 2. Log in to the Operations Manager and add the server as a **Metadata Server**. 3. Configure the metadata track using the Operations Manager. **To Disable:** • Use the Operations Manager to deactivate the service on the server. or • Use the Management Console to *Remove* the server from the Operations Manager, and then deselect the service.
VSF	Enables the Federator service used to monitor video and system health for the cameras and resources of multiple Operations Managers. The Federator service can only be enabled on a stand-alone server in this release. Other server services cannot be enabled on the same server as the Federator service. The Federator interface is accessed using a web browser or the Cisco SASD. Federator.	Activated using the Management Console only. Cannot be activated using the Operations Manager. **Note** This service is supported as a stand-alone server only, on a server running the RHEL 6.4 64 bit OS. **To Enable:** 1. Install the server and complete the Setup Wizard: select the **VSF** service. 2. Log in to the Cisco VSM Federator browser-based interface. and perform additional configurations. **To Disable:** • Log in to the Management Console and deselect the **VSF** service.

Related Documentation

- Cisco Video Surveillance Operations Manager User Guide
- Understanding Co-Located and Stand-Alone Servers, page 1-11

Understanding Co-Located and Stand-Alone Servers

Stand-alone servers are servers that run only a single server service.

Co-located servers are servers enabled with multiple server services, such as the Operations Manager and a single Media Server.

Some system configuration s require stand-alone servers. For example, the Cisco Video Surveillance Federator and Metadata services can only be run as stand-alone servers. In addition, Operations Manager HA requires that both servers in the redundant pair be stand-alone servers. Additional server services cannot be enabled.

Note Server services are the software packages that provide major functionality. See Understanding Server Services, page 1-8.

The following service combinations are supported in this release.

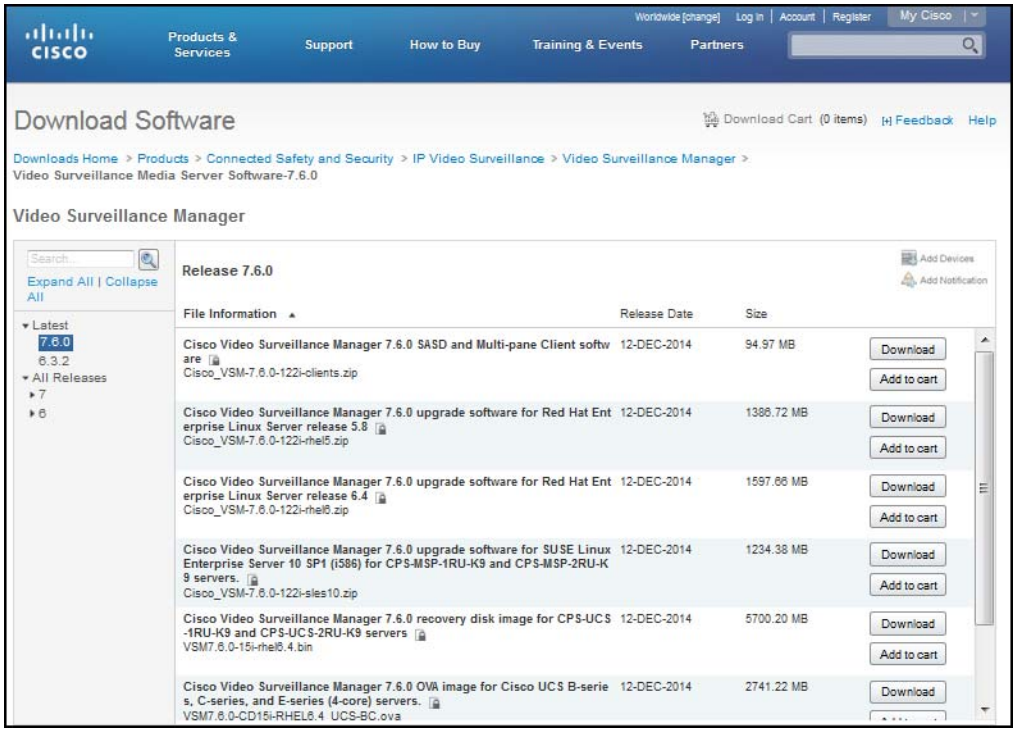
Table 1-6 Supported Server Service Combinations

Service	Supported Server Configuration
Operations Manager	Stand-alone server or co-located with one Media Server and/or one Maps server. • (Required) Each deployment requires one Operations Manager to manage the system. • Operations Manager HA configuration requires two stand-alone Operations Manager servers. • A co-located Operations Manager does not support the same number of Media Servers as a stand-alone Operations Manager.
Media Server(s)	(Required) Each deployment requires at least one Media Server to enable video streaming and recording. One Media Server can be co-located with the Operations Manager service. All additional Media Servers can be stand-alone servers or co-located servers with the Maps Server service. The following rules apply to co-located Media Servers: • Co-located Media Server can only be a primary Media Server (co-located Media Servers do not support other HA roles such as Standby or Redundant). • Failover or Redundant Media Servers cannot be associated with a co-located primary Media Server. Only a long term storage (LTS) server can be associated with a co-located primary Media Server. • Co-located Media Servers do not support the same number of cameras as a stand-alone server.
Metadata Server	(Optional) Stand-alone server only. Select the Service Type when adding the server to the Operations Manager configuration.
Maps Server	(Optional) Stand-alone server or co-located with the Operations Manager or a Media Server. Select the Service Type when adding the server to the Operations Manager configuration.
Federator	(Optional) Stand-alone server only. Select the VSF service using the Management Console Initial Setup Wizard. Other server services cannot be enabled on the same server as the Federator service.

Downloading Cisco Software, Firmware and Driver Packs

To download the Cisco VSM system software, device firmware, and driver packs, go to cisco.com (Figure 1-1).

Figure 1-1 Downloading Cisco Video Surveillance Software



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**—includes device driver packs for RHEL and SUSE servers.
- **Video Surveillance Manager Stand-alone Tools**—includes updates, plug-ins, and other resources.
- **Video Surveillance Media Server Software**—includes system software, OVA images, and SASD client software.

Step 4 Select the release (Figure 1-1).

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

Migrating from Cisco VSM Release 6.3.x

To migrate an existing release 6.3.x system, you must first migrate the servers and data from Cisco VSM 6.3.2 MR2 and 6.3.3 to Cisco VSM 7.2.x, and then upgrade the system to the latest release:

1. Contact your Cisco representative for assistance and instructions.
2. Migrate the system from Cisco VSM 6.3.2 MR2 or 6.3.3 to Cisco VSM 7.2.x.
3. Upgrade all physical and virtual Cisco VSM servers to Release 7.6 using the Cisco VSM Management Console.

Tip The migration procedure requires assistance from a Cisco representative. Contact your Cisco representative for more information.

Recovering or Reinstalling the Factory Image

You can create a recovery flash drive for Cisco Video Surveillance Manager (Cisco VSM) servers that contains a recovery image used to restore the server operating system, or return the server to the factory state, if needed.

Related Documentation

For instructions and more information, see the Cisco Video Surveillance Manager Recovery Guides for your release.

Recovery guides are available for the following:

- Release 7.2.0 and higher—Cisco Connected Safety and Security UCS series servers (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9).
- Release 7.0.0—Cisco Physical Security Multiservices platform servers (CPS-MSP-1RU-K9, CPS-MSP-2RU-K9) shipped with Cisco VSM 7.0.
- Release 6.3.2—Cisco Physical Security Multiservices platform servers (CIVS-MSP-1RU, CIVS-MSP-2RU and CIVS-MSP-4RU)

Deploying a Physical Cisco VSM Server

There are two ways to deploy a new Cisco VSM server:

- Physical server—Cisco VSM is pre-installed on new installations of the Cisco Connected Safety and Security UCS Platform Series (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9) when ordered with the Cisco VSM software installed. See the Cisco Connected Safety and Security UCS Platform Series User Guide.
- Virtual Machine—see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.

To deploy Cisco VSM on a physical server, refer to the following topics:

- Install a Physical Cisco VSM Server: Summary Steps, page 2-1
- Complete the Initial Setup Wizard, page 2-2

Install a Physical Cisco VSM Server: Summary Steps

Procedure

Step 1 Order and install the physical Cisco Connected Safety and Security UCS series server as described in the Cisco Physical Security UCS Platform Series User Guide.

For additional server hardware documentation, see the Cisco UCS C-Series Server Documentation Roadmap.

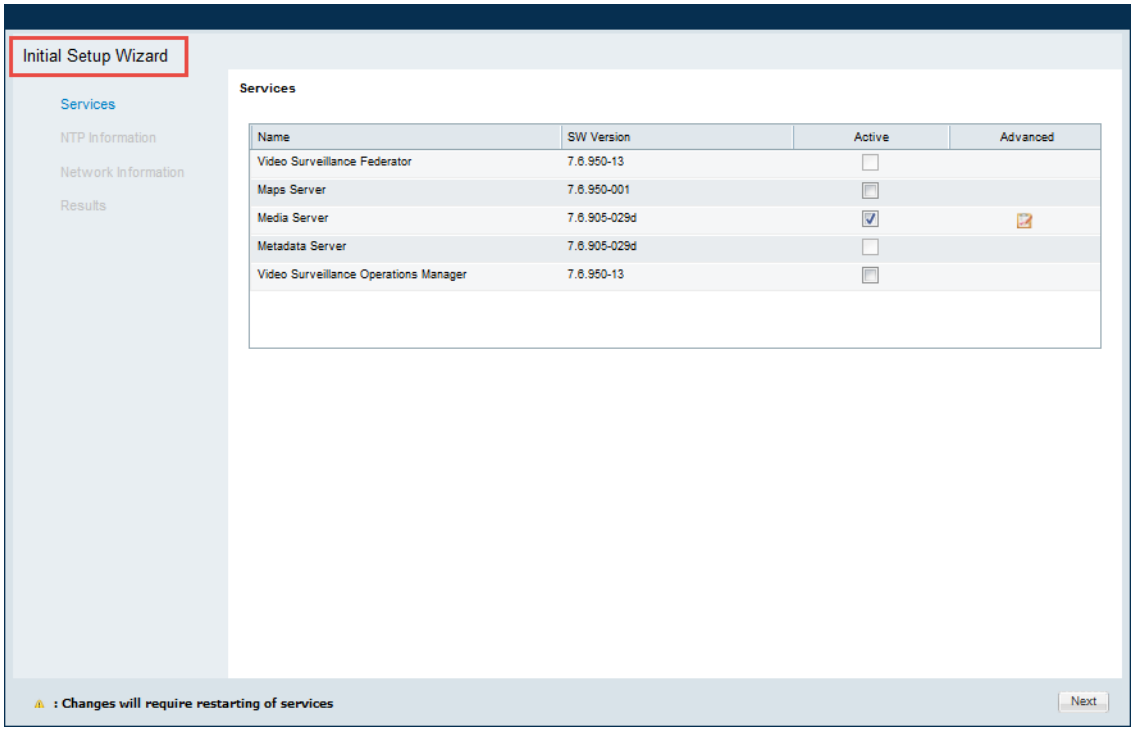
Step 2 Continue to Complete the Initial Setup Wizard, page 2-2 to perform the one-time Cisco VSM setup.

Step 3 Refer to the Cisco Video Surveillance Operations Manager User Guide for additional configuration and operation tasks.

Complete the Initial Setup Wizard

When you access a Cisco VSM server for the first time (by entering the IP address or hostname in a web browser), you are automatically redirected to Initial Setup Wizard (Figure 2-1).

Figure 2-1 Initial Setup Wizard



Follow the on-screen prompts to enter or accept the basic settings such as the server services, NTP source, and network settings. You may be prompted to restart the server services when the wizard is complete to activate the changes.

- Some fields require server services to restart when the wizard is complete.
- ✓ —Appears when a step is completed.
- Click **Back** to return to the previous step to revise or correct entries, if necessary.

Note This wizard only appears once. Future log-ins display the Management Console or the Cisco VSM Operations Manager.

Procedure

Step 1 Launch the 32-bit version of Internet Explorer on your Windows computer.

See the Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification for the complete workstation requirements.

Step 2 Enter the server URL.

The syntax is: **http://**<*server-ip-address or hostname*>**/vsmc/**, where the server address is one of the following:

Physical servers	The default (factory) static IP address is 192.168.0.200 For example, the URL is **http://192.168.0.200/vsmc/**
Virtual Machines: Cisco Unified Computing System (Cisco UCS) platform	The Cisco VSM server includes two network ports with the following default configuration: See the "Configuring the Network Settings" section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Step 3 Enter the Cisco VSM Management Console password.

Platform	Username / Password
Physical servers	• The default username **localadmin** is read-only and cannot be changed. • The default password is **secur4u**.
Virtual Machine—Cisco USC platform	• The default username **localadmin** is read-only and cannot be changed. • A new password is entered during the VM setup. See the "Changing the Default Password" section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Step 4 Click **Log In**.

Step 5 Enter and re-enter a new password.

Step 6 When the Initial Setup Wizard appears, select the *Services* that will run on the server, and click **Next**.

See the "Understanding Server Services" section in the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 7 Revise the *NTP* server and timezone, if necessary, and click **Next**.

See the "NTP Information" section in the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 8 Enter the *Network Information* (IP address used by network cards), if necessary, and click **Next**.

See the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 9 Click **Finish** and wait for the Wizard results to appear.

Step 10 Click **Reboot**, **Restart**, **or Close** when prompted.

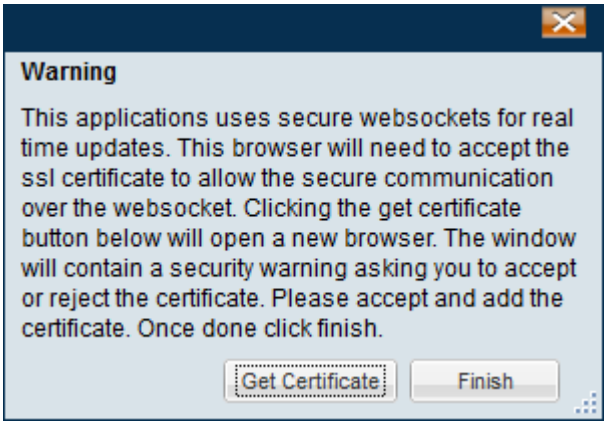
Restarting services can take up to 90 minutes or more depending on number of devices managed by the Operations Manager and Media Server. Installed products will be offline during this time.

Step 11 (Optional) Re-login to the Management Console, if necessary, to perform additional configuration or administrative tasks.

a. Re-login when prompted.

b. (Firefox browser only) Click **Get Certificate**, when prompted.

Figure 2-2 Firefox Browsers: Get Certificate Prompt



See the Cisco Video Surveillance Management Console Administration Guide for more information.

Step 12 (Recommended) Use the Operations Manager browser-based interface for most additional tasks, including server upgrades, network and NTP settings, and other tasks. See the Cisco Video Surveillance Operations Manager User Guide for more information.

Related Documentation:

- Cisco Video Surveillance Management Console Administration Guide
- Cisco Video Surveillance Operations Manager User Guide
- Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms

Upgrading System Software

Use this guide to update the system software on all servers, including the Operations Manager server and any additional servers (such as Media Servers or Metadata servers).

Note The Software Management page described in this document is supported in Cisco VSM Operations Manager release 7.5 and higher. For earlier releases, see the Cisco Video Surveillance Operations Manager User Guide for your release.

Contents

Refer to the following topics for more information:

Related Information

- Understanding Cisco Video Surveillance Software, page 1-5

Overview

Cisco VSM releases 7.2.x and higher can be upgraded using a `.zip` upgrade file that includes all required software packages. Installing the `.zip` file upgrades all components and ensures that all packages are running the required versions.

Always upgrade using the Cisco VSM user-interfaces. Do not perform the upgrade using the Linux CLI.

- Release 7.2 and earlier—Use the browser-based Management Console. See Cisco Video Surveillance Management Console Administration Guide for your release.

Note To upgrade from Release 7.2.0 or lower, you must first upgrade to Release 7.2.1 or higher, and then upgrade to the latest release. See the Release Notes for your release deployment for more information.

- Release 7.5 and later—Use the Software Management page on the browser-based Operations Manager to upgrade all of the servers in your deployment.

Note

- 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 and higher was pre-installed on the Cisco Connected Safety and Security UCS Platform Series (CPS-UCS-1RU-K9 and CPS-UCS-2RU-K9).
- Virtual Machine (VM) installations can also be upgraded as described in this document.

Upgrade Procedure Overview

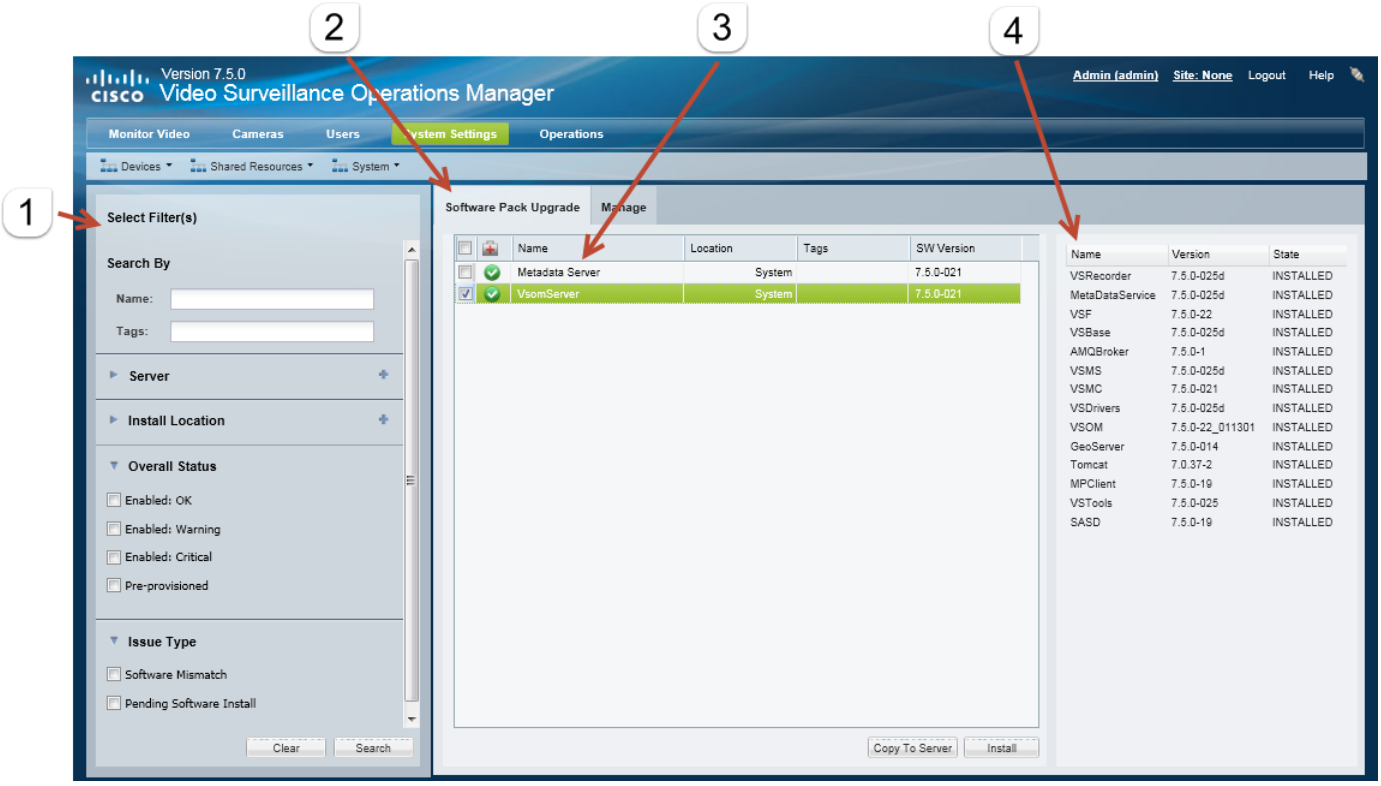
To upgrade the servers in your deployment, upload the software upgrade image to the Operations Manager, and then copy that software to the other servers that are managed by the Operations Manager. You can upload a single image for each operating system (OS), such as Red Hat or SUSE, but all servers must be upgraded to the same Cisco VSM release.

After the software upgrade image is uploaded, install in first on the Operations Manager server, and then on the additional servers as described in Server Upgrade Sequence, page 3-4.

Note The Software Management feature is supported in Cisco VSM release 7.5 and higher.

Figure 3-1 describes the main elements used to manage system software. See the "System Software Upgrade Procedure" section on page 3-5 for more detailed instructions.

Figure 3-1 Software Management



1	Filters used to narrow the displayed servers. Select the filers and click **Search**. Leave all fields blank to find all servers.
2	• **Manage**—Used to upload the new software upgrade `.zip` package to the Operations Manager server. • **Software Pack Upgrade**—Displays the servers discovered when you click **Search** (use filters to narrow the results). – Click **Copy To Server** to copy new software files from the Operations Manager server to the selected servers. You can copy the upgrade package to the servers before upgrading. – Click **Install** to install the software on the selected servers. **Tip** See the "System Software Upgrade Procedure" section on page 3-5 for more information.
3	The servers included in the search.
4	The software packages installed on the selected server. **Note** All required packages are included in the system software `.zip` installation file. The packages cannot be installed individually.

Server Upgrade Sequence

Cisco VSM servers should be upgraded in the following recommended order (depending on server type) to maximize access to video, minimize downtime, and ensure the integrity of video and configuration data.

1. Federator server
2. Operations Manager server
3. Map Server (if installed as a stand-alone server)
4. Failover Media Servers
5. Primary Media Servers
   a. Servers acting as Dynamic Proxy servers
   b. Servers not acting as Dynamic Proxy servers
   c. Redundant Media Servers
6. Long-term Storage Media Servers
7. Metadata Server

Usage Notes

- The Operations Manager and all associated servers must run the same system software version.
- The Operations Manager server must be in maintenance mode to perform the update (click the pencil icon in the title bar to turn maintenance mode on or off). The icon is grey when maintenance mode is on, meaning most user configuration will be rejected (only video access, system tasks, and logging are allowed).
- The SLES10, RHEL5, and RHEL6 operating systems (OS) are supported in this release. You must obtain and upload the correct software image for the OS running on each of the servers in your deployment. For example, if the Operations Manager server is running SLES10, but the Maps Server is running RHEL6, you must obtain and upload both files. When the files are copied from the Operations Manager to the server, the server OS is detected and the appropriate software image is transferred (as long as it is available on the Operations Manager).
- Only one software file per OS can be present on the server. If a new software file is uploaded, then the old file for that OS is deleted.
- To update a Federator server, log in to the Federator server.
- To repair or restore the Cisco VSM system software, see the Cisco Video Surveillance Manager Recovery Guide for your hardware platform. For VM installations, see the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms).
- Upgrading the server software may also require camera or encoder firmware upgrades. Failure to upgrade device firmware can cause camera failure after the server upgrade is complete.
  - See the Release Notes for Cisco Video Surveillance Manager for information on the supported firmware versions.
  - See the "Upgrading Cisco Camera and Encoder Firmware" section on page 5-1 instructions to upgrade Cisco device firmware.
- In rare scenarios, a PC workstation firewall can cause the upgrade process to fail. If this occurs, temporarily disable the workstation firewall software until the upgrade is complete.

- The server upgrade process automatically restarts server services.
- Installation is supported only if the RAID is in a non-bad, non-failed state.
- See Upgrading Language Packs, page 7-1 to manage the language packs on servers in your deployment.

System Software Upgrade Procedure

Use the following procedure to upgrade all of the servers in a deployment to the same Cisco Video Surveillance Manager release. See Server Upgrade Sequence, page 3-4 for the order in which the upgrade should be performed (by server type).

You can upload the server software to all servers before performing the upgrade.

Procedure

Step 1 Obtain the new software pack from the Cisco website.

- You must obtain and upload the correct software image for the OS running on each of the servers in your deployment. See the "Usage Notes" section on page 3-4 for more information.

  See the following for more information:

- Downloading Cisco Software, Firmware and Driver Packs, page 1-12.
- Release Notes for Cisco Video Surveillance Manager

Step 2 Log in to the Cisco VSM Operations Manager.

- You must belong to a User Group with manage permissions for *Servers and Encoders*. For more information, see the Cisco Video Surveillance Operations Manager User Guide.

Step 3 Click the pencil icon in the title bar to place the server in maintenance mode.

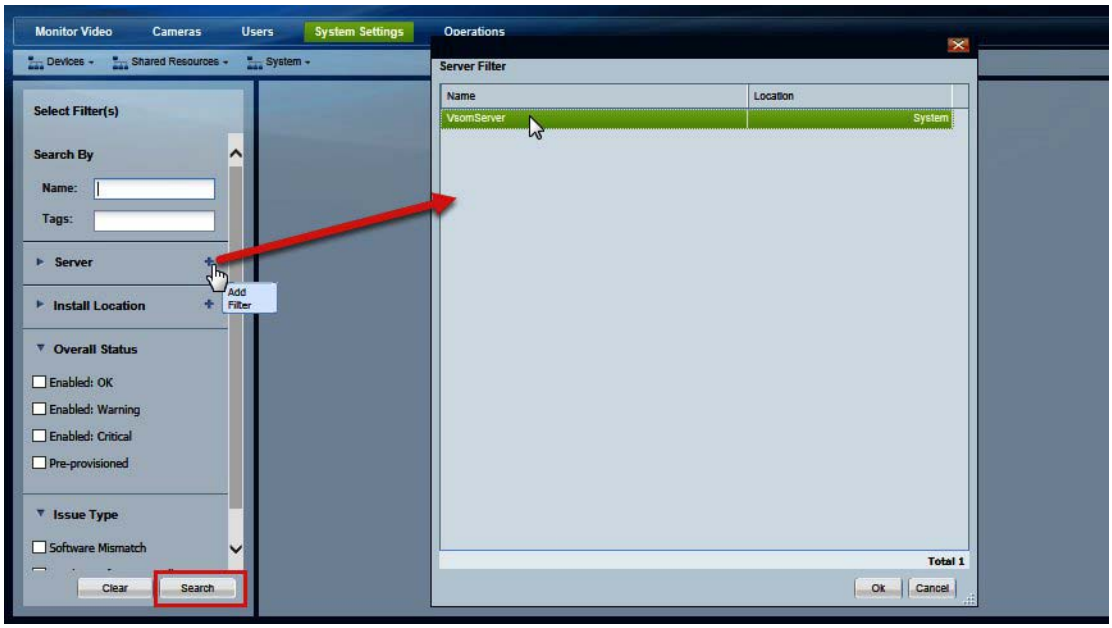
- The icon is grey when maintenance mode is on, meaning most user configuration will be rejected (only video access, system tasks, and logging are allowed).
- Maintenance mode locks the server configuration so configuration changes cannot be made by other users. This keeps the server config in a stable state during the upgrade.

Step 4 Upload the new software file(s) to the Operations Manager server.

Only one software file for each server operating system (OS) can be present on the server. If a new software file is uploaded, then the old file for that OS is deleted. See the "Usage Notes" section on page 3-4 for more information.

a. Select **System Settings > Software Management** (Figure 3-2).

Figure 3-2 Display the Server to Upgrade

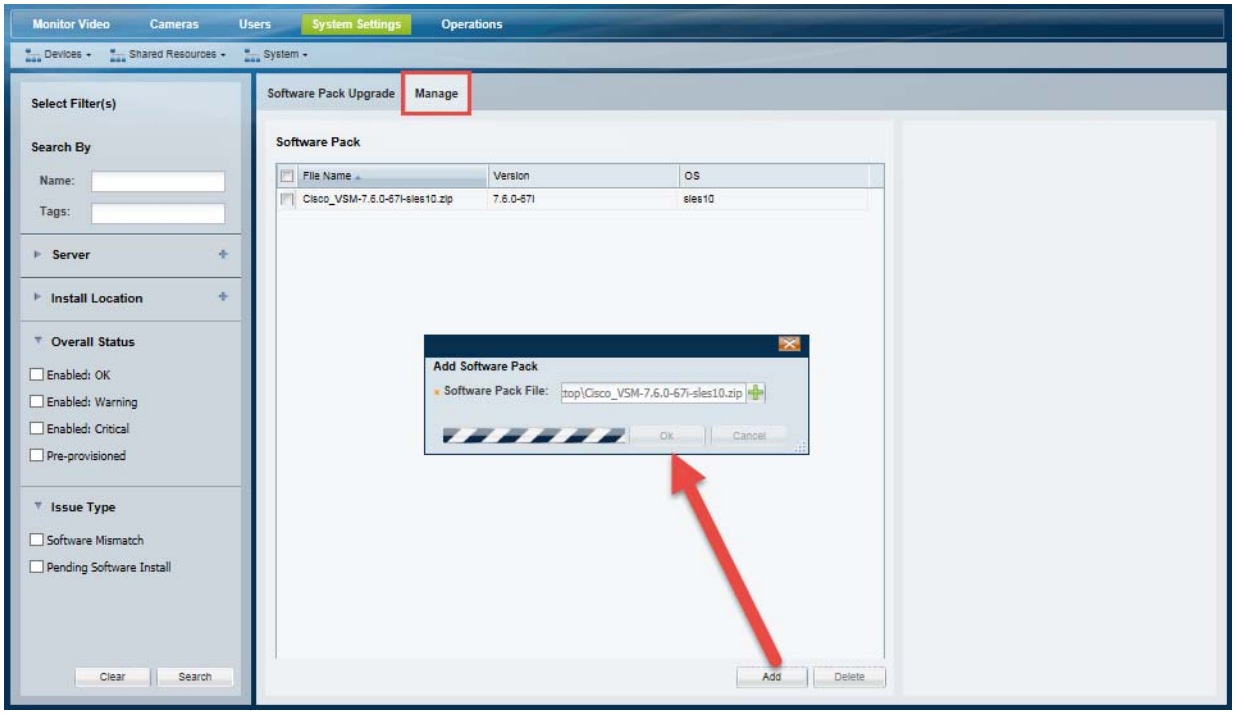


b. (Optional) Select the search filter(s), such as location or status.

c. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

d. Select the **Manage** tab (Figure 3-3). The **Manage** tab appears only after a server is selected.

Figure 3-3 Display the Server to Upgrade



e. Click **Add**.

f. In the pop-up window, click and select a valid `.zip` software pack file from a local or network disk. For example: `Cisco_VSM-7.6.0-1-sles10.zip`

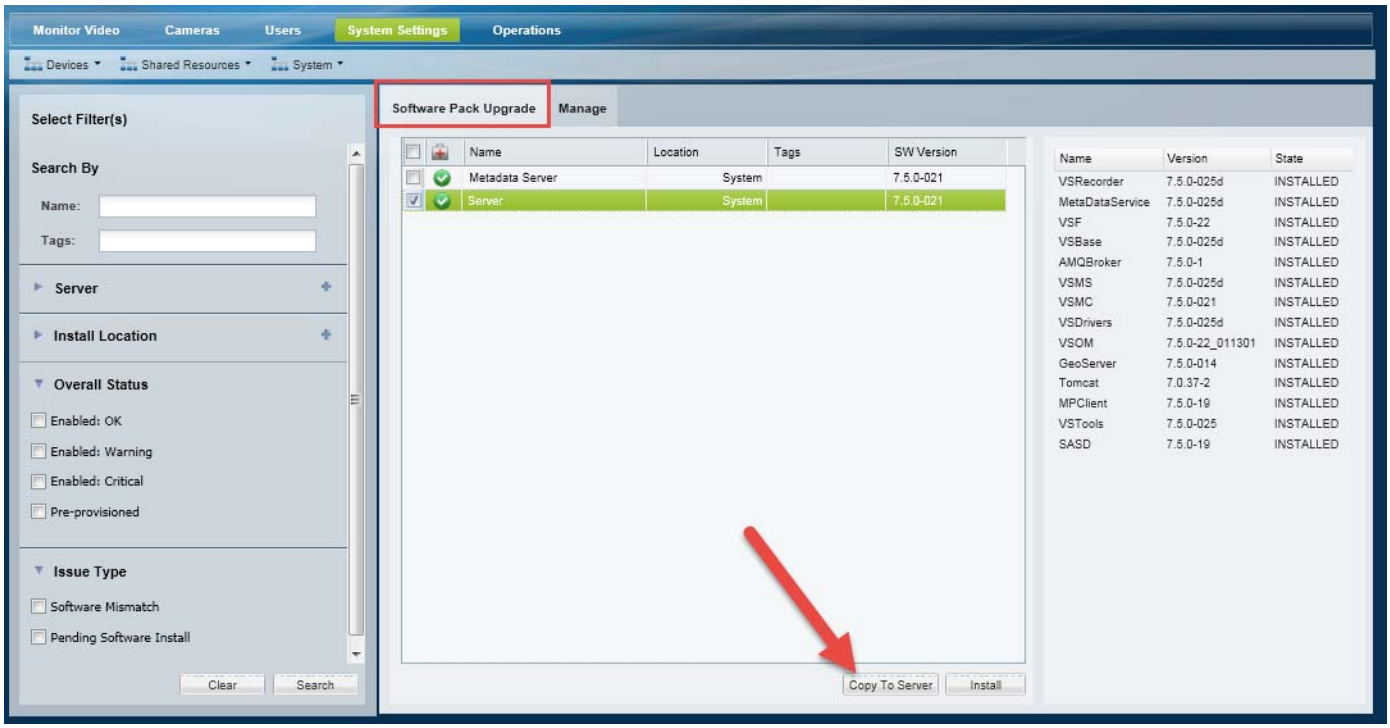
g. Click **OK**.

h. Wait for the software file to upload to the Operations Manager server. The filename will be displayed in the Software Pack list (Figure 3-3).

Step 5 Copy the upgrade software to the other servers that are managed by the Operations Manager (Figure 3-4).

Copying the software files to the other servers allows those servers to be upgraded. You can copy the software to the servers without installing it. This allows you to stage the software on all of the servers before performing the upgrade.

Figure 3-4 Copy the Software to the Additional Servers



a. Select the **Software Pack Upgrade** tab.

b. Make sure that maintenance mode is on (the icon is grey when maintenance mode is on).

c. (Optional) Use the filters to narrow the list of servers.

d. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

e. Click **Copy To Server** (Figure 3-4) to copy the new server software from the Operations Manager server to the selected server(s).

f. Wait for the file copy job to complete.

Step 6 Install the new software on the Operations Manager server.

Upgrade the Operations Manager before updating the other servers. See Server Upgrade Sequence, page 3-4.

a. Verify that the correct software file for the Operations Manager OS is uploaded (see "Usage Notes") and that maintenance mode is on (the icon is grey).

b. Select the Operations Manager server from the **Software Pack Upgrade** tab.

   For example: `VsomServer`.

c. Click **Install** to install the system software package that was copied to the server.

d. Wait for a series of status messages to appear while the status server is prepared and the upgrade package is extracted and verified.

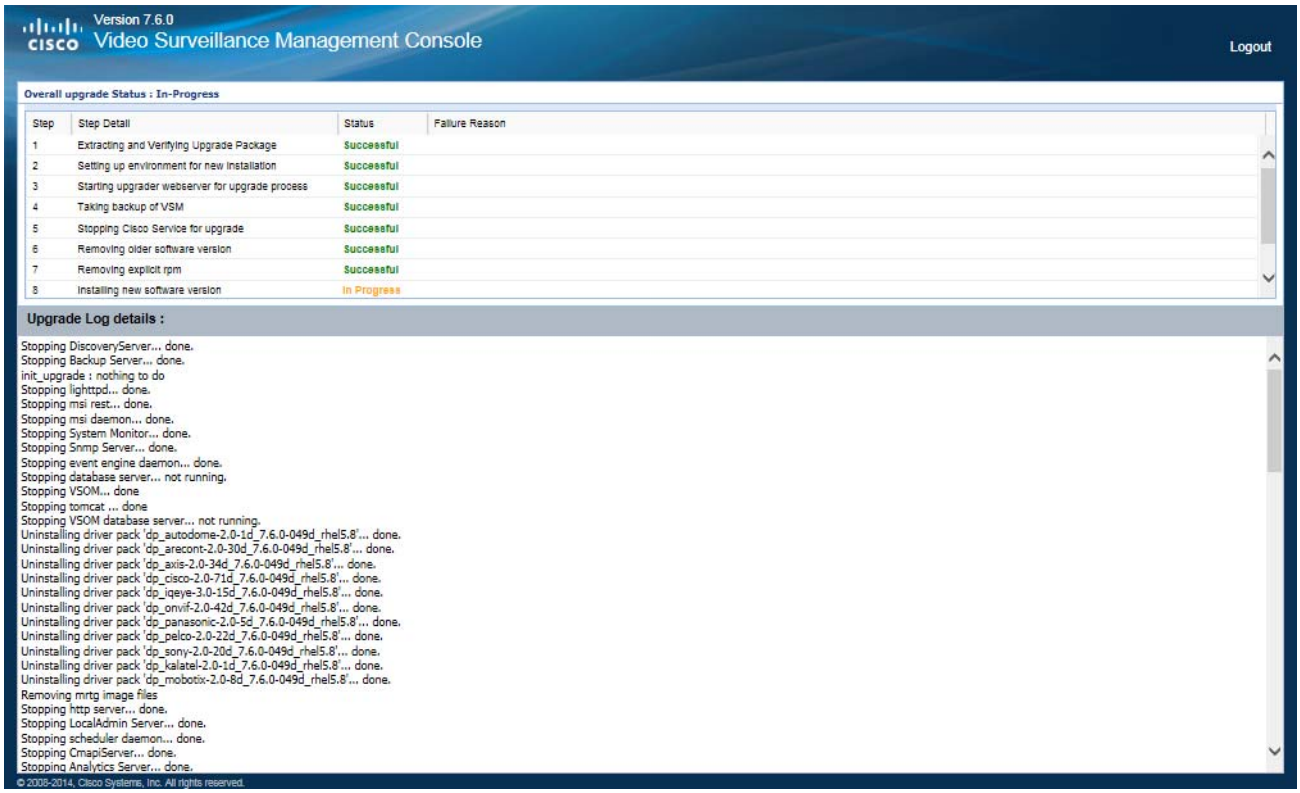
   This can take a few minutes.

e. (Optional) Re-login, when instructed, using the localadmin username and password (the credentials used for the Cisco VSM Management Console) to view the Operations Manager upgrade status.

   - Click **OK** when prompted to log in.
   - Enter the password for the localadmin username.
   - View the Operations Manager upgrade status (Figure 3-5).

Note To view this same status window for any server being upgraded to Release 7.6 or later, log in to the Cisco VSM Management Console. To view the upgrade status of additional servers using the Operations Manager, open the server configuration page, select **Status > Service Jobs** and select **Upgrade Server** from the menu (Figure 3-7).

Figure 3-5 Server Upgrade Status



f. Wait for the operation to complete and the server to restart. This can take up to 90 minutes (or less) depending on the server load.

g. Re-login to the Operations Manager, when instructed (you may need to refresh the browser to display the Operations Manager login page).

h. Continue to Step 7 to upgrade each additional server to the same version that is running on the Operations Manager.

Note If the upgrade fails, see the "Recovering From a Failed Upgrade" section on page 3-11.

Step 7 Install the new software on the additional servers that are managed by the Operations Manager (Figure 3-6).

a. Re-login to the Operations Manager (you may need to refresh the browser to display the Operations Manager login page).

b. Make sure that maintenance mode is on (the icon is grey when maintenance mode is on).

c. Verify that the software upgrade file was copied from the Operations Manager to the servers that will be upgraded, as described in Step 5.

d. Select **System Settings > Software Management**.

e. Select the **Software Pack Upgrade** tab.

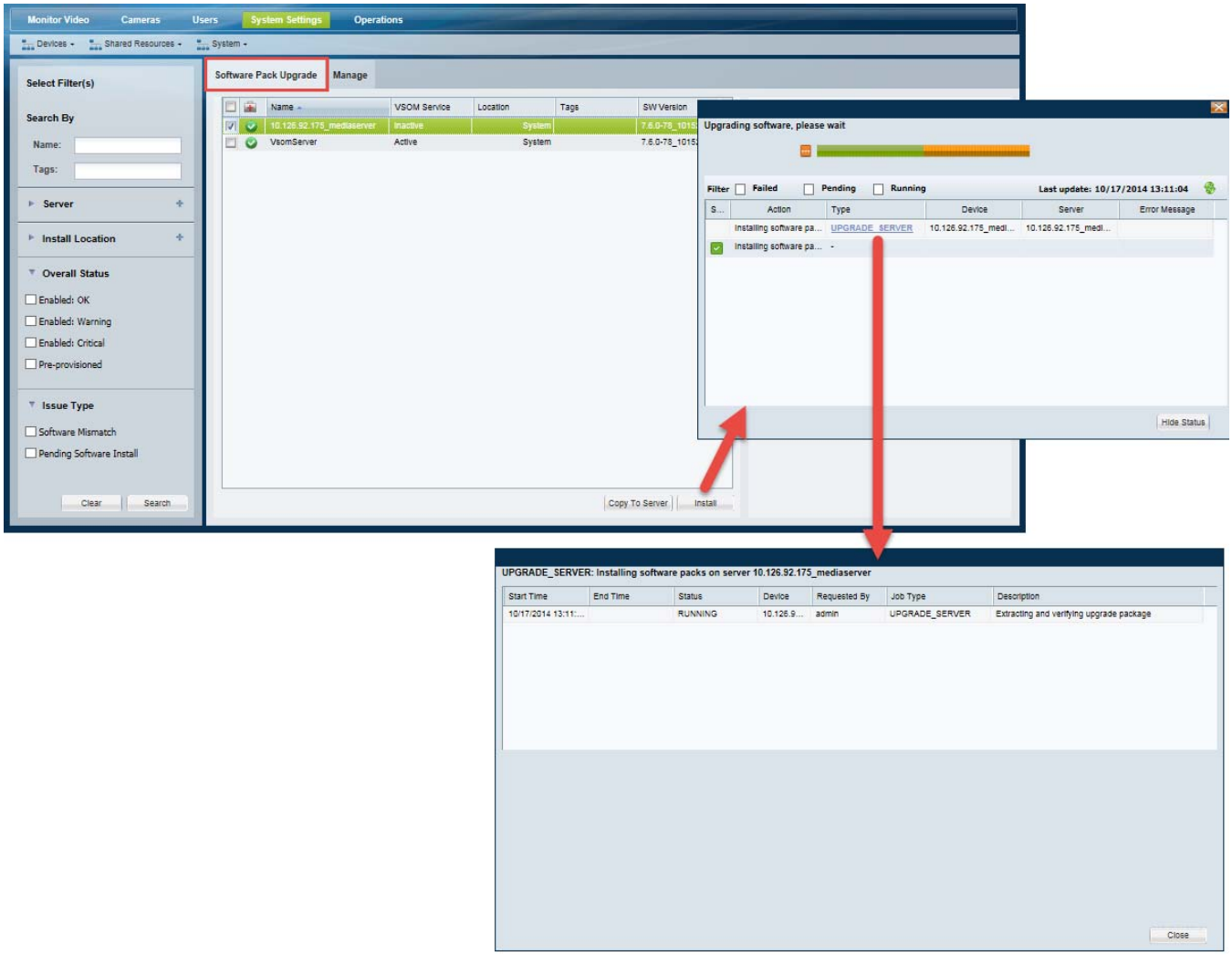
f. (Optional) Use the filters to narrow the list of servers.

g. Click **Search** to display the list of servers according to the filters. All servers are displayed if no filters are selected.

h. Select one or more servers from the list.

i. Click **Install** to install the system software package (Figure 3-6).

Figure 3-6 Upgrading Additional Servers



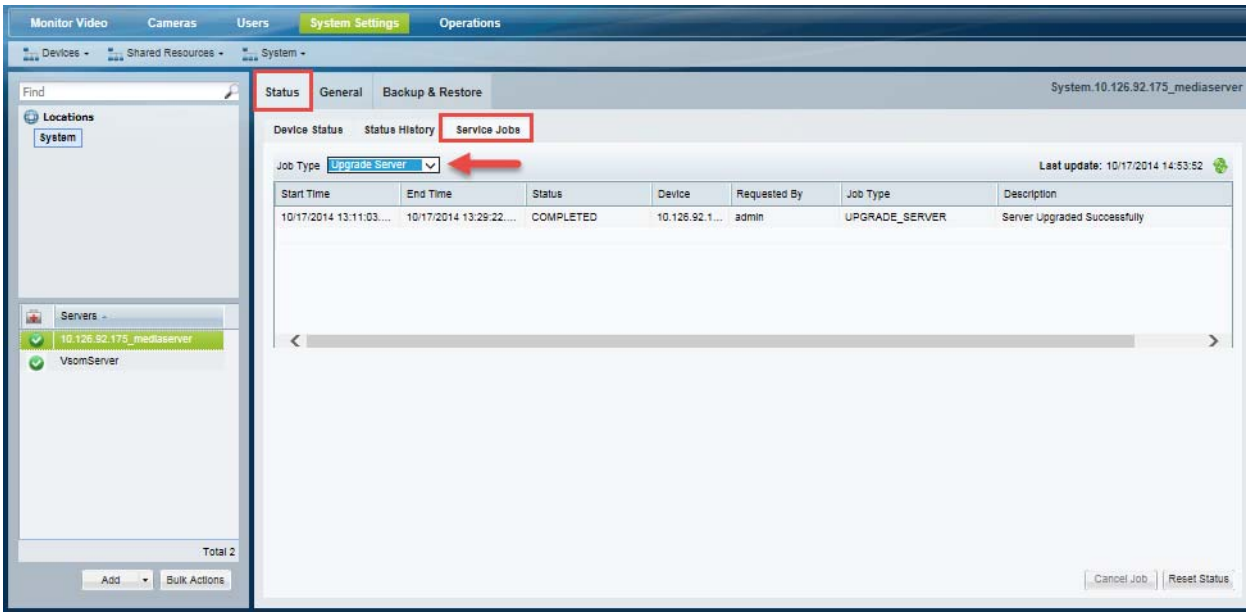
j. (Optional) In the Job window pop up window, click the “UPGRADE SERVER” link to view the job details.

k. Wait for up to 90 minutes for the upgrade job to complete and the server(s) to restart.

l. (Optional) View the upgrade job details (Figure 3-7):

- Go to **Devices** > **Servers** and select the server.
- Select the **Status** tab.
- Select the **Service Jobs** tab.
- Select the **Upgrade server** job type.

Figure 3-7 Server Upgrade Status



Note If the upgrade fails, see the "Recovering From a Failed Upgrade" section on page 3-11.

Recovering From a Failed Upgrade

If the upgrade fails or is interrupted, an error message ("work order file exists") may appear when you attempt to perform the upgrade again. This can be caused by a corrupted or incomplete upgrade file.

To address this issue, do the following:

Procedure

Step 1 Resolve the issue that caused the upgrade to fail. For example:

- Make sure the upgrade file is complete and not corrupted. Re-download the file again, if necessary.
- Make sure the upgrade can complete without interruption.

Step 2 Log in to the Cisco VSM server that was being updated and execute the server clean-up script.

Note This script cleans up the system so the upgrade can be attempted again. The script does not resolve the specific issue(s) that caused the upgrade failure. Resolve the cause of the upgrade failure first before attempting it again.

a. Log in using the *localadmin* username and password (the same credentials used to access the Cisco VSM Management Console).

b. Enter the following command to perform the server cleanup:

```
[localadmin@linux:~ ]# sudo /usr/BWhttpd/upgrade/server/bin/upgrade_cleanup.sh
```

Step 3 Repeat the System Software Upgrade Procedure, page 3-5.

Deleting a Software Pack File

To delete a software pack that was copied to the Operations Manager server, do the following:

Step 1 Select **System Settings > Software Management**. (Figure 3-1).

Step 2 Select the **Manage** tab.

Step 3 Select a software pack file name.

Step 4 Click **Delete**.

Installing and Upgrading Driver Packs

Device *driver packs* are the software packages used by Media Servers and the Operations Manager to interoperate with video devices. Driver packs are included with the Cisco VSM software, or may be added to a server to support new devices.

- Install new driver packs to add support for additional devices.
- Upgrade existing driver packs to enable support for new features.

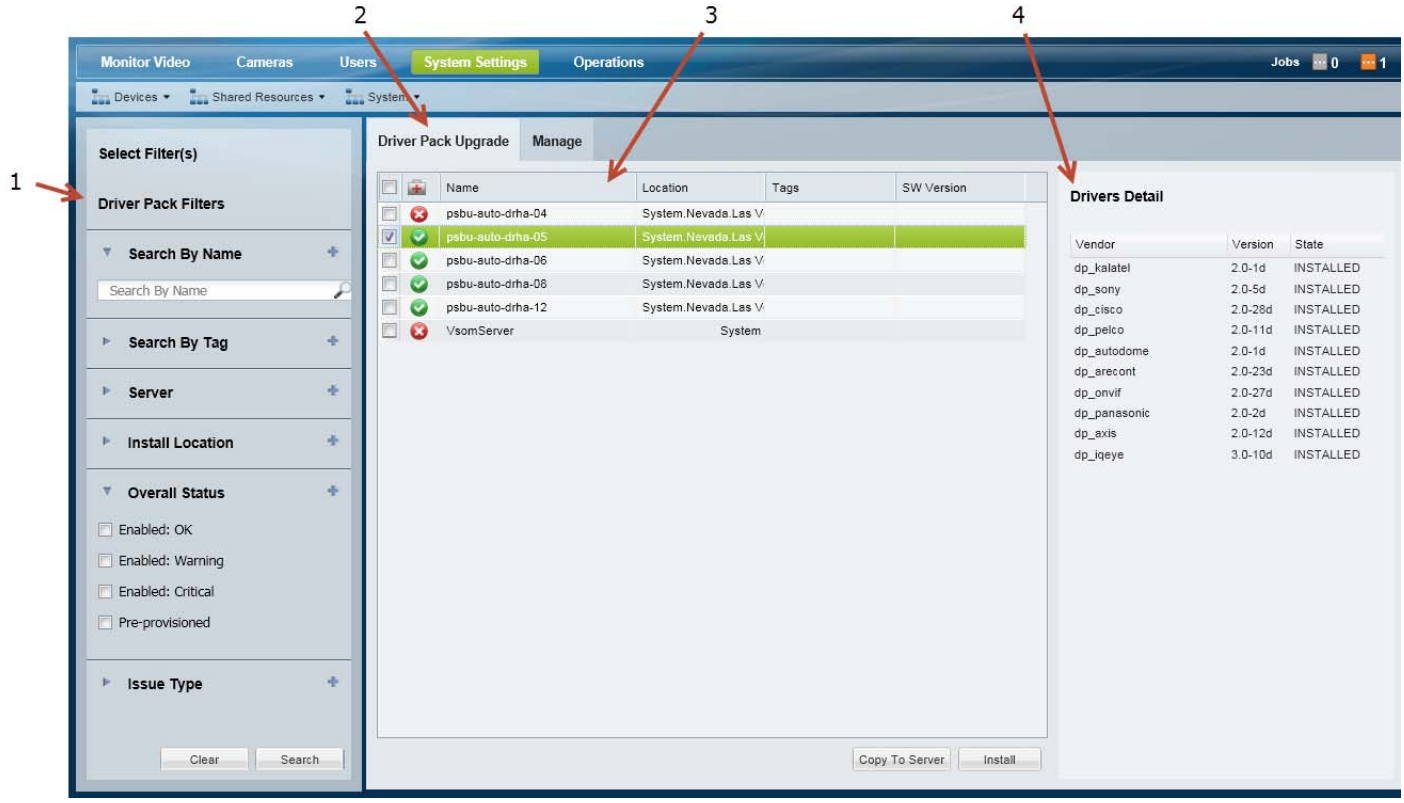
Refer to the following topics for more information:

Tip See the "Understanding Cisco Video Surveillance Software" section on page 1-5 for descriptions of the different software types.

Overview

Figure 4-1 describes the main elements used to manage driver pack software. See the "Driver Pack Upgrade Procedure" section on page 4-3 for more information.

Figure 4-1 Manage Drivers



1	Filters used to narrow the displayed servers. Select the filers and click **Search**. Leave all fields blank to find all servers.
2	• **Manage**—Used to copy new driver packs to the Operations Manager server. • **Driver Pack Upgrade**—Displays the servers discovered when you click Search (use filters to narrow the results). – Click **Copy To Server** to copy new driver files from the Operations Manager server to the selected servers. – Click **Install** to install all copied driver pack files on the selected servers. **Tip** See the "Driver Pack Upgrade Procedure" section on page 4-3 for more information.
3	The servers included in the search.
3	The driver packs installed for the selected server.

Usage Notes

- Driver packs must be upgraded to the same version on each server where the Media Server and Operations Manager services are enabled. For example, if your deployment includes a stand-alone Operations Manager, the Operations Manager server must have the same driver pack versions as the Media Servers associated with that Operations Manager. If the versions are different, a *driver pack mismatch* error can occur, which prevents camera template revisions.
- When driver packs are updated on Cisco VSM release 7.5 and later, only cameras and encoders using that driver pack are restarted. The Media Server and other devices are not affected.
- The driver pack file format is *.zip*. For example: `dp_cisco-2.0-28d_7.2.0-12d_sles10-sp1.zip`
- See the Release Notes for Cisco Video Surveillance Manager for information on the supported driver packs in your release.
- Driver packs can only be upgraded. They cannot be downgraded.

Driver Pack Upgrade Procedure

Step 1 Obtain the new driver pack from the Cisco website.

See the following for more information:

- Downloading Cisco Software, Firmware and Driver Packs, page 1-12.
- Release Notes for Cisco Video Surveillance Manager

Step 2 Select **System Settings > Driver Pack Management**. (Figure 4-1).

Step 3 Display the servers to be upgraded.

a. (Optional) Select the filter(s) to display specific servers.

Tip All servers are displayed if no filters are selected.

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

c. Select a server to display the driver packs installed on that server.

Step 4 Upload a new driver pack software file to the Operations Manager server.

a. Select the **Manage** tab (Figure 4-1).

b. Click **Add**.

c. In the pop-up window, click and select a valid *.zip* driver pack file from a local or network disk. For example: `dp_sony-2.0-15d_7.5.0-035d.zip`

d. Click **OK**.

e. Wait for the drivers to upload to the Operations Manager server.

The driver pack status is “Not Installed”.

Step 5 Copy the new driver packs from the Operations Manager server to the other servers.

Note Copying the driver packs to the other servers allows the Media Servers to be upgraded.

a. Select the **Driver Pack Upgrade** tab (Figure 4-1).
b. Select one or more servers.
c. Click **Copy To Server**.
a. Select the **Manage** tab.

Note You can copy the driver packs to the servers without installing them. This allows you to stage the software on a server without performing the upgrade, if necessary.

Step 6 Install the new driver packs on the servers.

Note Copying the driver packs to the other servers allows the Media Servers to be upgraded.

a. Select one or more servers from the **Driver Pack Upgrade** tab.
b. Click **Install** to install all driver packs that were copied to the server.

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

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

CHAPTER 5

Upgrading Cisco Camera and Encoder Firmware

Firmware for Cisco cameras and encoders can be upgraded using the Operations Manager as described in the following procedure. You can upgrade a single device, or multiple devices at a time.

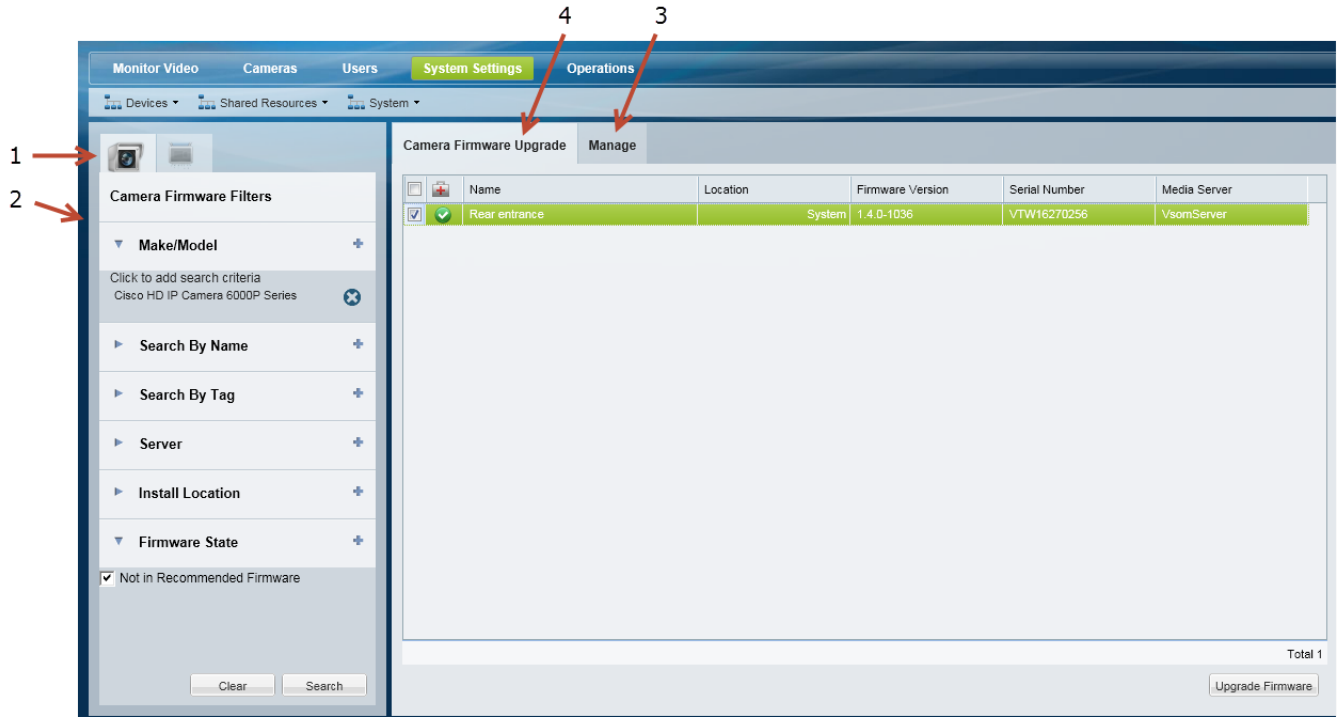
Refer to the following topics for more information:

Note Firmware for non-Cisco cameras is upgraded using a direct connection and the device user interface. See the device documentation to upgrade or downgrade the device firmware directly on the device.

Firmware Management Overview

Figure 5-2 describes the main elements used to manage firmware. See the "Upgrade the Cisco Device Firmware" section on page 5-3 for more information.

Figure 5-1 Firmware Management



1	Camera and Encoder tabs—Click to select the device type you want to manage.
2	Device filters—Select a Make/Model to enable the other filter fields and manage the device firmware.
3	Manage—Used to upload firmware images to the server, which can them be installed on the camera or encoder.
4	Firmware Upgrade—Used to upgrade specific devices that were discovered using the filter search.

Tip See the "Understanding Cisco Video Surveillance Software" section on page 1-5 for information about firmware, driver packs and system software.

Usage Notes

- Upgrade firmware for non-Cisco devices using a direct connection. See device documentation for more information.
- The Cisco devices must be available on the network and enabled in Cisco VSM. If the device is not available to Cisco VSM, connect directly to the device and upgrade the drivers (see the device documentation for instructions).

- The firmware image file must be a valid file format. Because the file format is different for each camera vendor, the Operations Manager will initially accept any file format, even if invalid. However, invalid files will cause the upgrade or downgrade to fail after 2-3 minutes.
- The upgrade can fail if device configuration changes are in process when the upgrade begins. If a device configuration is started during the upgrade, then the configuration change can fail. To avoid this, verify that no device configuration changes are running or started during the firmware upgrade (open the device **Status** page; the *Jobs in Progress* field should be *No*).
- The firmware version column in the *Manage* tab is only shown after the firmware has been applied to a set of devices.
- Each Media Server can update five devices at a time.
- Only one upgrade can be executed at a time. Wait until all devices are upgraded before initiating a new request.
- The vendor and device list includes the models that support firmware upgrades using the Operations Manager.
- To downgrade device firmware, select a previous version (the device must support downgrades).

Before You Begin

Before you begin, obtain the driver firmware for your device(s).

- To obtain firmware for Cisco devices, see Downloading Cisco Software, Firmware and Driver Packs, page 1-12.
- To obtain firmware for non-Cisco products, go to the product website or contact your sales representative.
- Verify that the firmware version is supported for your Cisco Video Surveillance Manager version. See the Release Notes for Cisco Video Surveillance Manager.

Upgrade the Cisco Device Firmware

Step 1 Download the firmware image from the Cisco website or device manufacturer.

See the following for more information:

- Downloading Cisco Software, Firmware and Driver Packs, page 1-12.
- Release Notes for Cisco Video Surveillance Manager

Step 2 Choose **System Settings > Firmware Management**.

- You must belong to a User Group with manage permissions for *Cameras* and *Images*.

Step 3 Select the camera  or encoder  tab (Figure 5-1 on page 5-2).

Step 4 Use the filters to select camera (Figure 5-1).

a. Select a Make/Model from the Filters to enable the other fields and the **Search** button

b. Expand the **Make/Model**.

c. Click the entry field.

d. Select the camera model from the pop-up list.

e. Select additional filter criteria, if necessary.

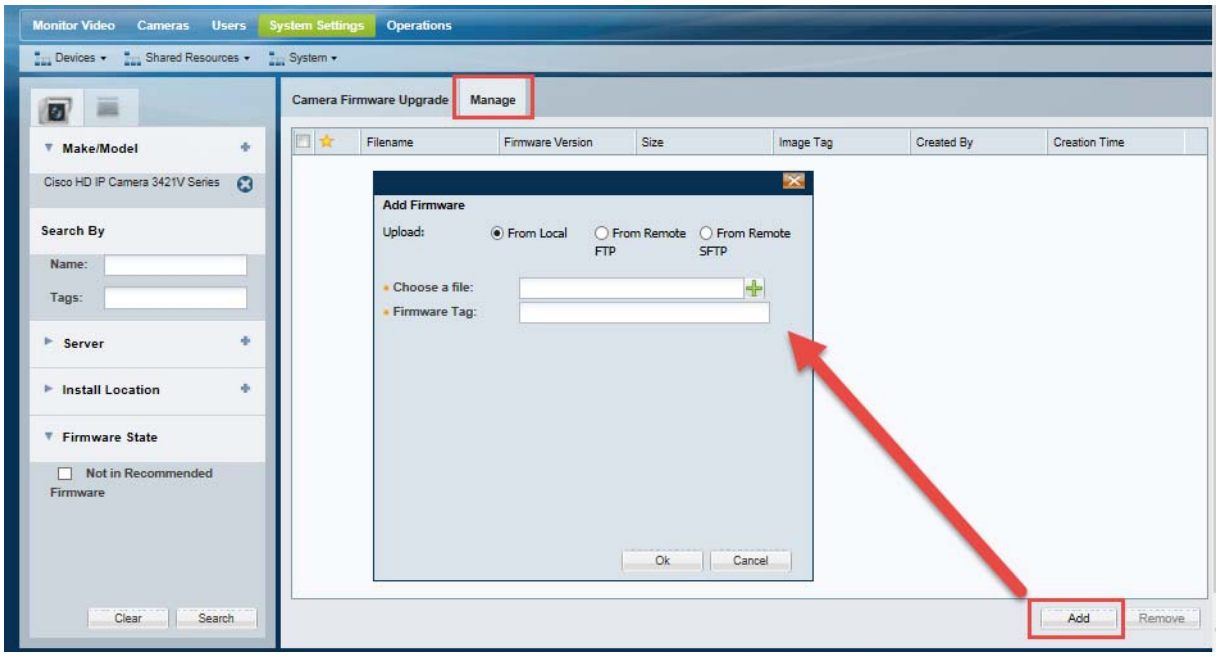
f. Click **Search**.

Step 5 (Optional) Add additional filter criteria to refine the search.

You can also click the **Make/Model**. field again to add additional device models.

Step 6 Add the firmware images (Figure 5-2):

Figure 5-2 Adding Firmware Images



a. Select the **Manage** tab.

b. Click **Add**.

c. Select the image location:

- **From Local**—Click ✚ to select the location of the firmware file
- **From Remote FTP—**enter the FTP connection details and remote file path. Click **Test** to verify the connection.
- **From Remote SFTP—**enter the FTP connection details and remote file path. Click **Test** to verify the connection.

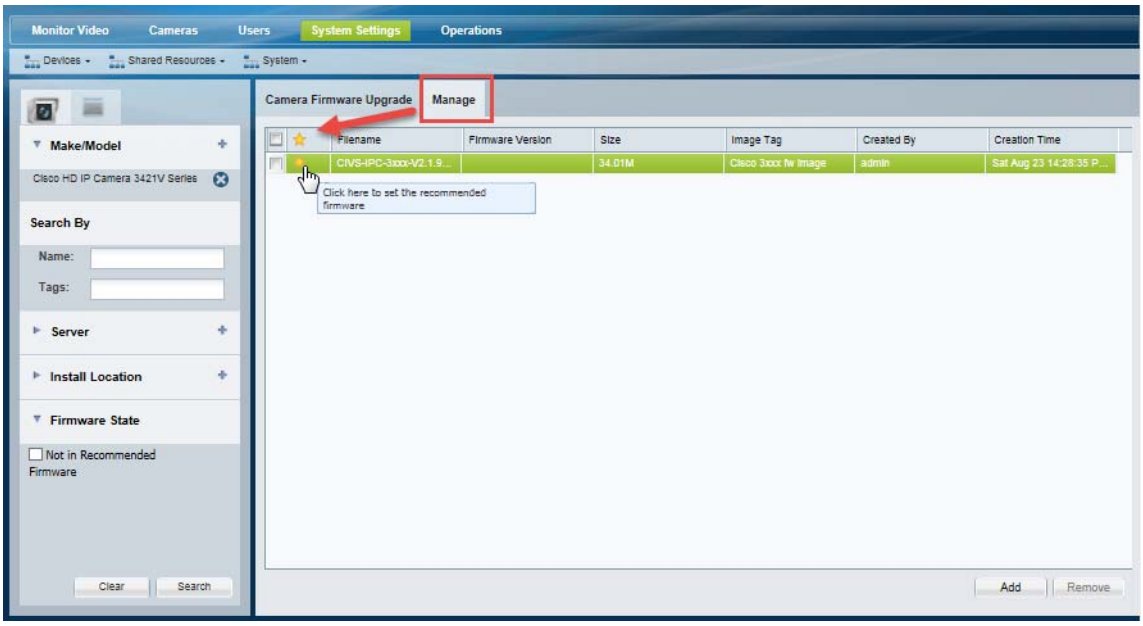
d. Enter a firmware tag that includes the firmware device model.

e. Click **OK**.

f. Wait for the file to upload and click **OK** when the success message appears.

Step 7 In the firmware list, select the star ★ next to a firmware image that is the recommended version for the device model. This firmware image will be used in the upgrade/downgrade (Figure 5-3).

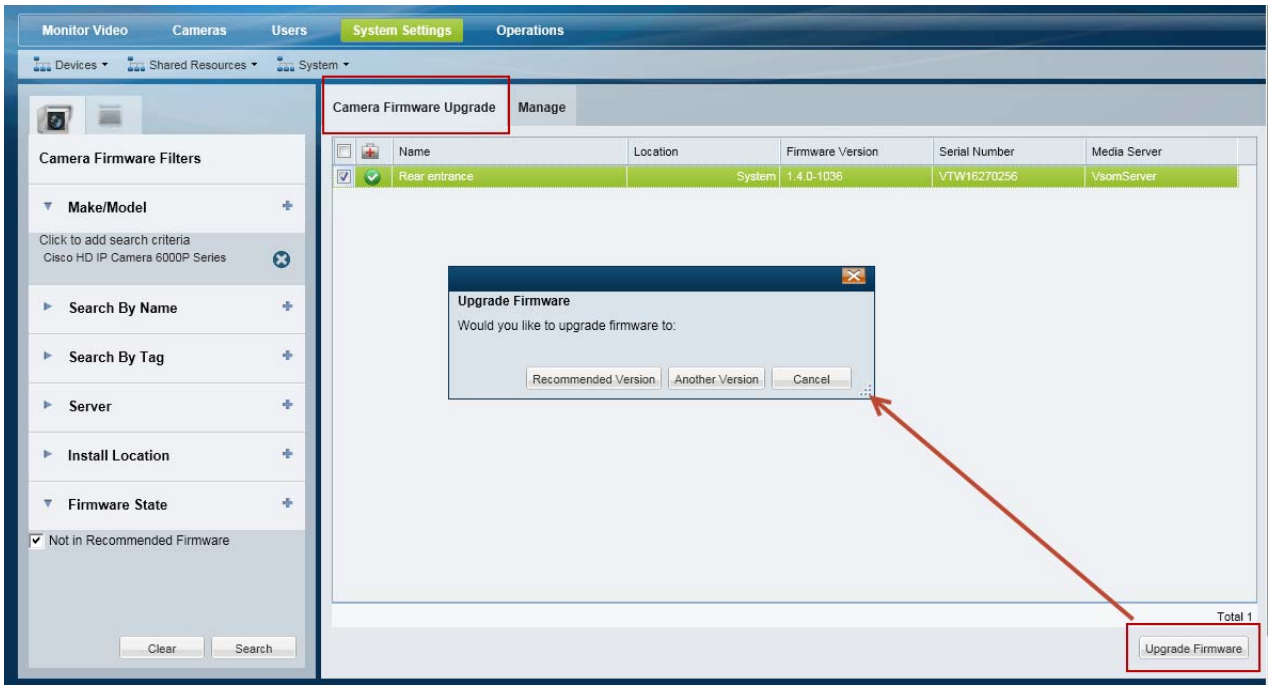
Figure 5-3 Adding Firmware Images



Note The Firmware version column is only displayed after the firmware has been applied to a set of devices.

Step 8 Upgrade the device firmware (Figure 5-4):

Figure 5-4 Upgrading Firmware



Note The firmware image file must be a valid file format for the camera model (for example: `CIVS-IPC-6xxx-V1.3.2-8.bin`). Although the Operations Manager will initially accept an invalid file format, the upgrade or downgrade will fail after 2-3 minutes.

Tip Select the filter **Firmware State > Not in Recommended Firmware** to view only the devices that do not have the recommended firmware version (as defined by the star ⭐ in Step 6).

Tip You can also downgrade devices by selecting a previous version, if the device supports downgrades.

a. Select the **Camera Firmware Upgrade** tab (or **Encoder Firmware Upgrade** tab).

b. Select the devices to be upgraded.

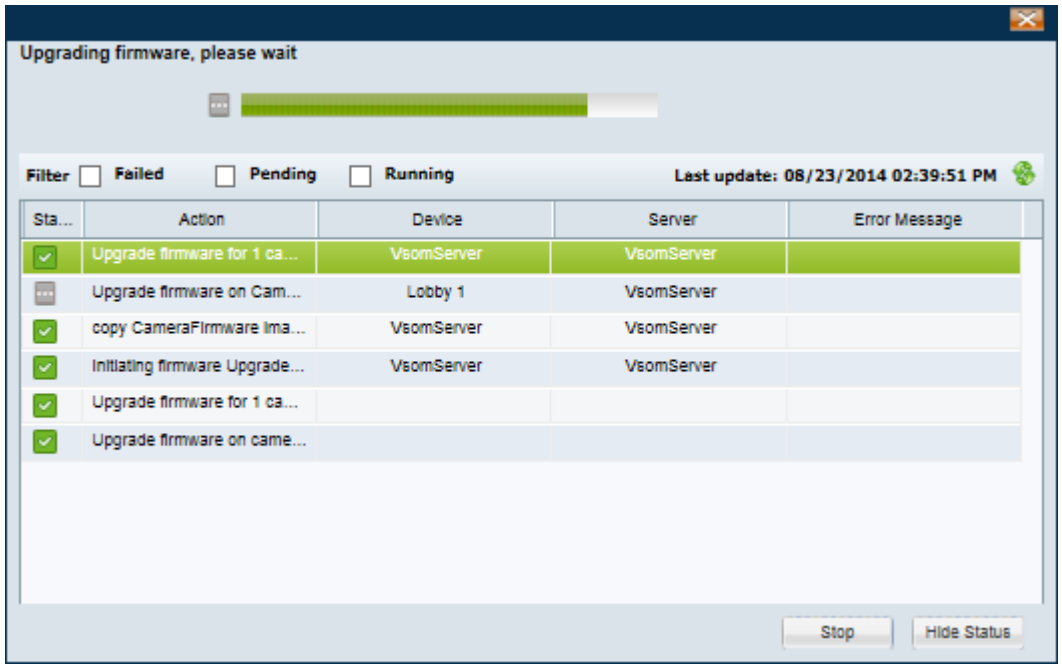
c. Click **Upgrade Firmware**.

d. Click **Recommended Version** or **Another Version**.

- **Recommended Version**—upgrade using the firmware version defined by the star ⭐ in Step 6. If no version was selected, then you must select a firmware version for the upgrade.
- **Another Version**—select the firmware version for the upgrade.

Step 9 Wait for the upgrade job to complete (Figure 5-5). See the "Usage Notes" section on page 5-2 if the upgrade is not successful.

Figure 5-5 Job Status



Installing Cisco Video Surveillance Safety and Security Desktop (Cisco SASD)

All Cisco SASD applications can be downloaded from cisco.com and installed on a monitoring workstation.

The Cisco SASD Advanced Video Player installer can also be downloaded from the browser-based Operations Manager (go to the **Operations** tab).

See the following for more information.

Understanding the Cisco SASD Application Suite

The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) is a suite of applications that allow Cisco Video Surveillance users to monitor live and recorded video. The suite includes the following components.

Table 6-1 Cisco SASD Applications

Application	Description
Cisco SASD	A full-featured monitoring application that provides access to the cameras and video from a single Operations Manager. Cisco SASD includes the following workspaces and features: • Video workspace • Wall workspace • Alert workspace • Maps workspace • Forensic Analysis Tools
Cisco SASD Advanced Video Player	An advanced monitoring application that includes the following monitoring workspaces: • Video workspace • Wall workspace
Cisco SASD Wall Launcher	Launches a monitoring application for unattended workstations. "Unattended" mode allows video monitoring windows to display Video Walls without access to the Cisco SASD configuration interface. The unattended screens can remain open even is the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation is rebooted.
Cisco SASD Wall Configurator	A utility for adding and modifying the video Walls that can be selected and displayed in the monitoring workstations.
Cisco SASD Federator	A monitoring application that allows Federator users to monitor video from multiple Operations Managers.

Tip For more information, see the Cisco Video Surveillance Safety and Security Desktop User Guide.

Installing the Cisco SASD Application Suite

All Cisco SASD applications can be downloaded from the cisco.com website. This includes all components described in the Understanding the Cisco SASD Application Suite, page 6-2.

Procedure

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

Step 2 Click Download Software.

Step 3 Select **Video Surveillance Media Server Software**.

Step 4 Select the release.

Step 5 Select the Cisco Video Surveillance Safety and Security Desktop application.

Step 6 Click **Download Software** next to the software package and follow the on-screen instructions.

Step 7 Locate and launch the installation file, and follow the onscreen instructions.

Step 8 Complete the on-screen instructions to install or upgrade the Cisco Multi-Pane Video Surveillance client software on your computer. This application is an Active X client that enables video playback and other features. Video will not play unless the Cisco Multi-Pane client software is correctly installed. You must have administrative privileges on the PC workstation to install the software.

Installing the Cisco SASD Advanced Video Player

The Cisco SASD Advanced Video Player application can also be downloaded from the browser-based Operations Manager.

Procedure

Step 1 Log in to the Cisco VSM browser-based Operations Manager.

a. Launch Internet Explorer on your Windows computer.

b. Enter the URL for the Cisco VSM Operations Manager.

c. Enter your username and password.

d. From the Domain menu, choose the default “localhost” if your account was created using the Operations Manager. Select a different Domain only if you are a user from an external database (Active Directory LDAP domain) and are instructed to do so by your system administrator.

e. Enter a new password if prompted.

Note You must enter a new username the first time you log in, or when your password periodically expires.

Step 2 Select the **Operations** tab (Figure 6-1).

Figure 6-1 Downloading the Cisco SASD Advanced Video Player Installer from the Operations Manager

Step 3 Click **Advanced Video Player** (under the *Software* heading).

Step 4 Follow the onscreen instructions to complete the installation.

Step 5 Complete the on-screen instructions to install or upgrade the Cisco Multi-Pane Video Surveillance client software on your computer. This application is an Active X client that enables video playback and other features. Video will not play unless the Cisco Multi-Pane client software is correctly installed. You must have administrative privileges on the PC workstation to install the software.

Tip

- To access the application on your workstation, go to **Start > SASD Video Player**.
- You can also double-click the Safety And Security Desktop icons on your desktop, or go to **Start > All Programs > Cisco Safety And Security Desktop**.
- You can save the installer file and use it to install the application on multiple workstations, if necessary. Users must have a valid Cisco VSM username and password to access the system.
- An error appears if the Microsoft .NET Framework 4.0 is not installed. Go to http://www.microsoft.com/en-us/download/confirmation.aspx?id=17851 to download the installer, then repeat this procedure.

Upgrading Language Packs

Add language packages to display the Cisco Video Surveillance interface in additional languages.

Language Settings

Language settings define the user interface language, the date and time formats, and the first day of the week. Modify the following settings as needed and click **Save**.

Table 7-1 Language Settings

Setting	Description
System Language	Select a supported language for the user interface text. To upload new or revised language packs, see Uploading Language Packs, page 7-2.
Date Format	Select the date format displayed in system messages, alerts, and other generated information. For example, **MM/DD/YYYY** means that dates will appear as month, day, and year. • d = day • M = Month • y = year
Time Format	Select the time format displayed in system messages, alerts, and other generated information. For example, **hh:mm:ss tt** means that the time will be displayed as hours, minutes, and seconds, and include the AM/PM notation. • hh = hour • mm = minute • ss = second • tt = A.M. or P.M.
First day of week	Select the day that should be considered the first day of the week. For example, **Monday**.

Uploading Language Packs

Add language packages to display the Cisco Video Surveillance interface in additional languages. You must upgrade the language packs on all servers in your deployment.

Procedure

Step 1 Download the language pack from the cisco.com (see Downloading Cisco Software, Firmware and Driver Packs, page 1-12).

Step 2 Upload the language pack:

a. Log in to the Cisco VSM Operations Manager.

b. Go to **System Settings > Language Settings > System Language**.

c. Click  and select the language pack from a local or network drive.

d. Click **Upload**.

Step 3 Select the language for the user interface:

a. After the system is restarted, login to the Operations Manager.

b. Go to **System Settings > Language Settings > System Language**.

c. Select the system language.

d. Click **Save**.

Cisco Video Surveillance Manager Recovery Guide

This document describes how to create a recovery flash drive for Cisco Video Surveillance Manager (Cisco VSM) Release 7.5 and higher, running on the Cisco Connected Safety and Security UCS Platform Series servers.

This bootable USB drive contains a recovery image that you can use to restore the operating system on a server, or restore the server to the factory state, if needed.

Tip Back up existing system data to a PC or FTP/SFTP server before performing the recovery to preserve system configuration and (optionally) historical data. See the Cisco Video Surveillance Operations Manager User Guide for instructions.

This document includes the following topics:

Supported Servers

The Cisco VSM Release 7.5 and higher recovery images are supported by the Cisco Connected Safety and Security UCS Platform Series servers, including the following:

- Cisco Connected Safety and Security UCS C220: CPS-UCS-1RU-K9
- Cisco Connected Safety and Security UCS C240: CPS-UCS-2RU-K9

Note Other server models and servers shipped with earlier versions of the Cisco VSM software are not compatible with the recovery process described in this document.

Creating a Recovery Flash Drive

This section describes how to create a recovery flash drive by obtaining the recovery image and placing it on a USB flash drive.

Requirements

The USB flash drive that you use must:

- Have a capacity of at least 8 GB
- Contain no files other than the recovery image files

Cisco recommends using USB memory sticks that are made by Kingston or SanDisk.

Procedure

Step 1 Insert a USB drive into a PC port (see Requirements, page 8-2).

Step 2 Download the recovery image on the Windows PC:

a. Go to the Cisco Video Surveillance Manager product page.

b. Click Download Software.

c. Select **Video Surveillance Media Server Software** (including system software).

d. Select the release.

e. Click **Download Software** next to the recovery file and follow the on-screen instructions.

Step 3 Download and install a utility used to raw write a binary image to a USB disk.

For example: see the **Win32 Disk Imager** download at:
http://sourceforge.net/projects/win32diskimager/files/latest/download

Step 4 Write the recovery image to the disk:

a. Launch the disk image utility and select the binary recovery file.

b. Select the destination USB drive.

c. Follow the utility instructions to create the recovery disk.

Step 5 Remove the USB stick from the Windows PC.

Recovering the Operating System from a Recovery Flash Drive

This section describes how to use a recovery flash drive to restore the operating system on a server.

Requirements: Before You Begin

Before you begin, do the following.

Note These tasks are important to ensure that your data is preserved and the recovery process is successful.

- Prepare a flash drive as described in the "Creating a Recovery Flash Drive" section on page 8-2.
- Disconnect any USB or external storage devices (including SAN storage) from the server.
- Installation is supported only if the RAID disks are in a non-bad, non-failed state.
- Back up existing system data on servers running services other than Media Server (such as Operations Manager, Federator, or Metadata).
  - Back up existing system data to a PC or FTP/SFTP server before performing the recovery. This allows you to restore system configurations and historical data.
  - See the Cisco Video Surveillance Operations Manager User Guide or Cisco Video Surveillance Management Console Administration Guide for instructions.

Procedure

To restore the operating system from a recovery flash drive, follow these steps:

Step 1 Complete the "Requirements: Before You Begin" tasks.

Step 2 (Servers running services other than Media Server) Back up existing system data to a PC or FTP/SFTP server before performing the recovery.

- Use the Operations Manager or Management Console UI to perform the backup.
- See the Cisco Video Surveillance Operations Manager User Guide or Cisco Video Surveillance Management Console Administration Guide for instructions.

Step 3 Power off the server on which you need to restore the operating system.

Step 4 Disconnect (unplug) any USB storage devices and any external storage (such as SAN storage connected through a fibre channel) that are connected to the server.

This ensures that only the recovery flash drive is attached to the server and prevents other storage devices from accidentally being cleared by the recovery process.

Step 5 Put the recovery flash drive in a USB port on the server and power on the server.

Step 6 When the Cisco logo appears, press the **F6** key to select the boot device.

Step 7 Select the USB recovery flash drive and press **Enter**.

Step 8 At the "boot>" prompt, type one of the following options and press **Enter**:

Table 1 Recovery Options

Recover Options	Option Description
recovery	Reinstalls the operating system. • Recorded video and configurations are preserved. • RAID configurations are preserved (only the OS partitions are formatted).
factory	Restores the server to the factory default settings: • Reinstalls the operating system • Clears and reconfigures the RAID. You must disconnect any external storage before using this option. • Recorded video and configurations are deleted **Caution** This action deletes all data and video files.
factory_raid5	Restores a Cisco Connected Safety and Security UCS C240 server to the factory default settings, including: • Reinstalls the operating system • Clears and reconfigures the RAID. You must disconnect any external storage before using this option. • Recorded video and configurations are deleted • Valid only on the Cisco Connected Safety and Security UCS C240 with 6 or 12 internal drives. **Caution** This action deletes all data and video files.
rescue	Boot to prompt from USB media. Use this option to recover a password or for other administrative tasks.

Tip To skip software re-installation remove the USB flash drive and reboot the server by pressing **CTRL+ALT+DEL** keys.

Note Ignore any "modinfo: could not find module megasar" errors that may occur during the installation. This does not impact the installation process.

Step 9 When the installation is complete, you are prompted to reboot.

Step 10 Remove the USB flash drive and reboot the server.

Step 11 Complete the Initial Setup Wizard (see Complete the Initial Setup Wizard, page 2-2).

Step 12 Use the Management Console UI to restore the configuration backups you created in Step 1. Restore your data based on the recovery method used:

- **Recovery** option—(Servers running services other than Media Server) When the Recovery option is used, restore only the CDAF (console) backup. This is because only the Media Server service is enabled after server comes back up. The configuration data is still present on the server for the other services, but you must restore the CDAF backup file to re-enable those services (that were running on the server prior to recovery).
- **Factory** options—Restore the server services in the following order:

Operations Manager Server	Stand-Alone Server (such as Media Server)	Federator Server
a. Management Console (CDAF)	a. Management Console (CDAF)	a. Management Console (CDAF)
b. Media Server (VSMS)	b. Media Server (VSMS)	b. Federator (VSF)
c. Operations Manager (VSOM)	c. Additional server services	
d. Additional server services		

Note CDAF runs on all servers and provides the Cisco VSM Management Console user interface and features. CDAF backups include the server database, system information, console jobs and other data. The CDAF service must be restored along with the other server services or information may be missing and system errors can occur.

Step 13 Log in to the Operations Manager UI and verify that your system configuration and video data is present.

Step 14 Use the Operations Manager to configure system, network, and related settings as appropriate for your deployment. For instructions, see the Cisco Video Surveillance Operations Manager User Guide

Related Documentation

Use one of the following methods to access the Cisco Video Surveillance (Cisco VSM) documentation:

- Click **Help** at the top of the screen to open the online help system.
- Download PDF versions at **Operations** > **Help**.
- Go to the Cisco Video Surveillance documentation web site.
- See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

Revision History

Table B-1 Revision History

Date	Change Summary
October, 2015	Updated recovery instructions to clarify requirement to backup and restore. See Recovering the Operating System from a Recovery Flash Drive, page 8-3.
April 2015	Initial draft. See the Release Notes for Cisco Video Surveillance Manager for more information.