Cisco Video Surveillance Manager: Design Guide

Cisco Video Surveillance Manager, Release 7.7

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.
CONTENTS

Preface ix

Obtaining Documentation and Submitting a Service Request ix

Overview

CHAPTER 1

Introduction 1-1

Overview  1-2

Understanding Cisco VSM Data Flow  1-4

Designing the Enterprise Network Infrastructure  1-4

Understanding Cisco VSM Servers and Server Services  1-5

Using Physical vs. Virtual Media Servers  1-5

Understanding Server Services  1-6

Understanding Co-Located and Stand-Alone Servers  1-7

Network (IP) and Analog Camera Support  1-8

Video Viewing Options  1-8

Monitoring Hardware Requirements  1-10

1-10

Best Practices

CHAPTER 2

Best Practices 2-1

General Best Practices Guidelines  2-1

Document Your System Before You Begin  2-3

Network Links  2-5

Network Reachability  2-5

Dual-Stream and Custom Configurations  2-5

VSM 7 Audio Support  2-6

Legality of recording  2-6

Prerequisites  2-6

Configuring Live and Recorded Audio  2-6

External Microphone Suppliers and Examples  2-7

Signal Levels from External Microphones  2-7
CHAPTER 3
Securing Cisco Video Surveillance Manager  3-1
  Controlling Physical Access  3-2
  Establishing a Secure Network Topology  3-2
  Changing Default Passwords  3-2
  Session and Password Timeouts  3-3
  Configuring Port Access for Cisco VSM  3-4
  Using Secure Remote Access  3-4
  Configuring User Roles and Access  3-4
  Administration and Monitoring Tools  3-5
  Logging Out from Management Console and Operations Manager  3-5
  Securing Client Systems  3-5

Deployment Considerations

CHAPTER 4
Deployment Scenarios  4-1
  Overview  4-2
  Deployment Scenarios  4-3
    Scenario 1: Centralized Data Center Architecture  4-3
    Scenario 2: Centralized Management, Distributed Architecture  4-4
    Scenario 3: Distributed Management, Distributed Architecture  4-5
  Additional Deployment Scenarios and Options  4-6

CHAPTER 5
Deployment Summary Steps  5-1

CHAPTER 6
Determining the Required Resources  6-1
  Factors That Determine Your Server Deployment Scenario  6-1
  Determine Bandwidth and Storage Estimates for Media Servers and Cameras  6-3
  Using the Guided System Selling Tool  6-4
  Methods to Reduce Video Bandwidth Usage  6-6

CHAPTER 7
Video Recording Options  7-1
  Summary of Recording Options  7-1
  Best Practices for Recording on Motion  7-2
  On-Camera Recording (Connected Edge Storage)  7-3
    Deployment Scenarios  7-3
      Network Bandwidth Savings  7-3
      Off-Network Cameras  7-4
Network Considerations

**Server and Camera Network Configuration** 8-1
- Summary of Network NAT Support 8-2
- Server Network Considerations 8-3
  - Network Port Requirements 8-3
  - Default Ethernet Interface Settings 8-3
  - Rules for Server Reachability 8-4
    - Dual-homed/NAT Configurations 8-4
  - Server Reachability 8-4
- Supported Ethernet Port Configuration Combinations 8-5
- Using Dynamic Host Configuration Protocol (DHCP) 8-6
  - Server DHCP 8-6
  - Camera DHCP 8-6
- DNS Server Support 8-7
- Network Settings in a Virtual Machine (OVA File) Installation 8-7
- Understanding Device Conflicts 8-7
  - Devices with Duplicate IP Addresses 8-7
  - Conflicts During Camera Discovery 8-8
  - Allowing Duplicate Camera IP Addresses 8-8
- Resolving ID Mismatch Errors When Changing Camera IP Addresses 8-9
  - Scenario 1: Cameras Configured with DHCP IP Addresses 8-9
  - Scenario 2: Cameras Configured with a Static IP Addresses 8-10
- Adding Cameras From Different Networks (NATs) 8-11
  - Overview 8-11
    - Understanding Camera IP Addresses 8-11
    - Understanding Camera IP Address Conflicts 8-13
    - Camera Discovery and IP Addresses Conflicts 8-14
    - Manually Adding Cameras 8-15
  - Camera Network Deployment Scenarios 8-15
    - Scenario 1: All Devices Are In the Same Network (NAT) 8-15
    - Scenario 2: Cameras in Different NATs Use Static Access IP Addresses 8-17
    - Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses 8-18

**Understanding NTP Configuration** 9-1
- Recommended (and Default) NTP Configuration 9-2
Server Features and Options

CHAPTER 10 Server Storage 10-1
- Storage Types: SAN (FC & iSCSI), NAS Considerations 10-1
- Extending Video Archive Retention Using Long Term Storage Servers 10-2

CHAPTER 11 Using Dynamic Proxy to Monitor Video From Low-Bandwidth Sites 11-1
- Dynamic Proxy Overview 11-1
- Dynamic Proxy Design Considerations 11-3
- Dynamic Proxy Frames to Skip 11-3
- Configuring Dynamic Proxy 11-4

CHAPTER 12 Server High Availability 12-1
- Operations Manager (VSOM) HA 12-1
  - Understanding Operations Manager HA 12-2
  - Requirements 12-4
- Media Server Redundancy and Failover 12-6
  - Understanding Redundant and Failover Servers 12-6
  - Understanding Media Server Failover 12-8
  - Requirements 12-9
  - Determining HA Server Scalability 12-10
  - Failover Server Recommended Load and Limitations 12-10

CHAPTER 13 Designing Virtual Machine Deployment on Cisco UCS Platform Servers and Blades 13-1
- Introduction 13-2
- Solution Components 13-4
- Logical Network Topology 13-5
- IP Network Infrastructure 13-6
- Performance and Scalability 13-9
- Storage Considerations 13-9
- Design Recommendations for Deployment Models 13-9
  - WAN Considerations 13-12
Example 1—Network Bandwidth Usage 13-13
Example 2—Sites with Remote Storage 13-15
Example 3—Distributed Media Servers 13-17

High Availability 13-19

Camera Discovery and Bulk Deployment

CHAPTER 14

Bulk Camera Configuration and Deployment 14-1
Adding Multiple Cameras 14-1
Importing Cameras from a List 14-1
Best Practices 14-2
Discovering Cameras on the Network 14-3
Applying Camera Settings to Multiple Cameras 14-3

CHAPTER 15

Discovering Cameras on the Network 15-1
Camera Discovery Options 15-2
Understanding Camera Conflicts During Discovery 15-3
Enabling the Auto Configuration Defaults for a Camera Model 15-4
Discovering Non-Medianet Cameras Using Bonjour 15-5
Cameras Pending Approval List 15-7
Discovering Medianet-Enabled Cameras 15-8
  Medianet Requirements 15-8
  Medianet Overview 15-10
  Configuring a DHCP Server with Option 125 15-12
  Medianet Camera Discovery Procedure 15-13
  High Availability Impact on Medianet Cameras 15-14

User Access

CHAPTER 16

Controlling User Access Permissions 16-1
Understanding User Access Permissions 16-2
Understanding the Impact of a User’s Location 16-3
Create a User Access Plan 16-3
More Information 16-5
  Understanding the System-Defined User Roles, Groups and Accounts 16-5
  Understanding Permissions 16-6
  Understanding the Super Admin 16-9
CHAPTER 17
Using Locations to Limit User Access 17-1
Overview 17-2
Summary Steps 17-2
Understanding Permission-Based and Partition-Based Resources 17-3
Simple Deployments (User Access to All Devices and Resources) 17-4
Permission-Based Resources: Limiting User Access to Devices 17-4
Partition-Based Resources: User Access to Templates, Schedules and Other Resources 17-5
Examples: Locations in Simple vs. Large Deployments 17-7

Video Events and Analysis

CHAPTER 18
Using Events to Trigger Actions 18-1
Understanding Events and Alerts 18-2
Health and Security Event Types 18-3
Triggering Actions Based on Alerts and Events 18-3

CHAPTER 19
Using Video Analytics for Post-Event Motion Detection 19-1
Configuring and Using Video Analytics 19-1
Network Design Considerations 19-1

Integrating External Systems

CHAPTER 20
Using ActiveMQ to Monitor Cisco VSM 20-1

CHAPTER 21
Using the Cisco VSM APIs and SDK 21-1
Understanding the Cisco VSM Software Development Kit (SDK) 21-2

APPENDIX A
Related Documentation A-1

APPENDIX B
Revision History B-1
Preface

Revised: August 21, 2015

The Cisco® Video Surveillance Manager (Cisco VSM) is an advanced security solution for enterprise organizations at a centralized location, or who have offices and sites at diverse geographical locations. This document provides an overview of features and options that should be considered when designing a Cisco VSM deployment. This includes network bandwidth and access, server type and location, camera features, mapping, analytics, metadata analysis, and more.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.
PART 1

Overview
Introduction

Cisco Video Surveillance Manager (Cisco VSM) is a comprehensive video surveillance system that enables security teams to collaborate effectively while managing thousands of cameras. Cisco VSM is highly scalable, secure, and policy-based.

This document introduces the main Cisco VSM components and features, and describes how to design and deploy Cisco VSM in a variety of scenarios.

Refer to the following topics for more information:

- Overview, page 1-2
- Understanding Cisco VSM Data Flow, page 1-4
- Designing the Enterprise Network Infrastructure, page 1-4
- Understanding Cisco VSM Servers and Server Services, page 1-5
  - Using Physical vs. Virtual Media Servers, page 1-5
  - Understanding Server Services, page 1-6
  - Understanding Co-Located and Stand-Alone Servers, page 1-7
- Network (IP) and Analog Camera Support, page 1-8
- Video Viewing Options, page 1-8
- Monitoring Hardware Requirements, page 1-10
Overview

Cisco VSM is a comprehensive video surveillance system that enables your network and security teams to collaborate effectively in a highly scalable environment combining both video and network techniques to optimize the experience. Cisco Video Surveillance Manager comprises several components that combine to create a flexible, highly scalable system for the enterprise.

Cisco Video Surveillance Operations Manager allows a user to quickly and effectively configure and manage video throughout the enterprise. It provides a highly secure web portal to configure, manage, display, and control video in an IP network, and allows you to easily manage a large number of security assets and users, including media servers, cameras, encoders, and event sources.

Cisco Video Surveillance Media Server, a core component of the Cisco Video Surveillance Manager, performs the distributed processing of all video, audio, and event information with N+1 redundancy at a camera-by-camera level. Collection and routing of video from a wide range of cameras and encoders over an IP network is another important function of the Media Server.

Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) is a suite of applications that allow Cisco Video Surveillance operators to monitor live or play back recorded video in single- or multipane views based on camera location or name. SASD also allows user to monitor, react, and manage alerts and events in association with cameras.

In summary, a Cisco VSM deployment includes the following main components (Figure 1-1):

- The network(s) where Cisco VSM is installed.
- The physical or virtual Cisco VSM servers that provide services to manage and record video, configure Cisco VSM features, display components on a map, generate metadata from existing video, and other features.
- The video cameras that capture live video and perform optional processing and storage.
- The monitoring workstations that allow operators and security personnel to view live and recorded video, configure features, perform analytic analysis, create and save video clips, and other features.
Figure 1-1  Cisco VSM: Main Components

- Cisco SASD (Desktop Application for monitoring video)
- Cisco Operations Manager (VSOM) (Browser-based UI for configuration and management)
- Custom Application (APIs are used to display and manage video in a customer application)

**Overview**

Users log in to the Operations Manager (VSOM) to configure resources, request video, or use features.

**Management Console (VSMC):**
(Browser-based) Initial server setup and server-specific management tools

**Operations Manager (VSOM):**
A single server that manages and configures Media Servers, cameras, VSM users and features

- Media Server (VSMS)
- Live and recorded video is managed by a Media Server

- Analog Camera
- Encoder
- IP (Network) Cameras

**Built-in features**

**Notifications, Triggers and Actions**

**Custom Programming**
Understanding Cisco VSM Data Flow

Cisco VSM data flows through the Cisco Media Server, not the Cisco VSM Operations Manager (Figure 1-2). Design your network and Cisco VSM deployment with that in mind.

Figure 1-2 Cisco VSM Data Flow

Designing the Enterprise Network Infrastructure

The enterprise network infrastructure where Cisco VSM is deployed is critical to system performance and reliability. In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support high-quality IP Video Surveillance. In other instances, network hardware might require upgrading or reconfiguration to support increased bandwidth needed to support video. Quality-of-service (QoS) techniques are important for any design because video has similar—in some instances, more stringent—requirements than VoIP for loss, latency, and jitter.

See the Cisco Video Surveillance Solution Reference Network Design Guide, Release 7 for high-level design recommendations and best practices for the enterprise network infrastructure where Cisco VSM is deployed.

Note

Issues may be encountered when using VSM with high latency network links such as data transmitted through satellite links. When the latency through the network from VSM to a camera exceeds 500 ms, problems may be experienced that are dependent on the model of the camera and the video mode in use. In particular, there are known issues when Economical Streaming mode is used with .1FPS video sent from a camera via a high latency network link to a remote VSM server. Please contact Cisco for recommendations on deployments requiring use of high latency network connections.
Understanding Cisco VSM Servers and Server Services

A Cisco VSM deployment includes one or more Cisco VSM servers that provide video processing, storage, analytics, configuration interface, monitoring, and other features.

- Using Physical vs. Virtual Media Servers, page 1-5
- Understanding Server Services, page 1-6
- Understanding Co-Located and Stand-Alone Servers, page 1-7

Using Physical vs. Virtual Media Servers

All servers can be deployed as physical appliances pre-installed with Cisco VSM, or a virtual machines (VMs) running on the Cisco Connected Safety and Security UCS series servers (Table 1-1).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine (VM)</td>
<td>An .OVA template file is installed on a supported Cisco UCS blade to create a new virtual machine (VM) instance of the server.</td>
<td>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.</td>
</tr>
</tbody>
</table>

The server functionality is the same in either format, although some performance differences and considerations apply. You can also combine physical and VMs in a deployment.

- Virtual machines are often used in a centralized deployment where multiple servers are installed in a central NOC. Although VM deployment requires some additional configuration during the initial setup, and additional maintenance of the VM platform, you can more easily manage multiple servers or add additional VMs as the needs of your deployment changes.
- Physical servers are frequently deployed at the edge, where only one or two servers are required to support the cameras in a location or LAN. Physical servers are pre-installed with the Cisco Video Surveillance Manager software.
Understanding Server Services

Each server can run one or more services that provide features and functions for the Cisco Video Surveillance system. For example, the Operations Manager provides the configuration interface and management features for the entire deployment, while the Media Server service manages cameras and encoders and plays and records video.

At a minimum, every Cisco VSM must include a Cisco VSM Operations Manager server and a Cisco Media Server. These services can be co-located on a single physical or virtual server, or installed on stand-alone servers.

Table 1-2 describes the server services supported on each physical or virtual machine.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Manager</td>
<td>The browser-based Cisco VSM Operations Manager administration and configuration tool. The Operations Manager be added as a stand-alone server, or co-located with other services (such as a Media Server and/or Maps Server).</td>
</tr>
<tr>
<td>Media Server</td>
<td>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 Media Servers can be added as a stand-alone server, or co-located with the Operations Manager, or co-located with the Operations Manager and the Maps service.</td>
</tr>
</tbody>
</table>
| 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.  
- This service is supported as a stand-alone server on a server running the RHEL 6.4 64 bit OS, or co-located on a Operations Manager server.  
- In co-located deployments, use the Operations Manager to activate the service. |
| 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. |
| 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. |
Understanding Co-Located and Stand-Alone Servers

Stand-alone servers are servers that run only a single server service. A stand-alone server can be a physical or virtual machine.

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

Some system configurations 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 1-6.

The following service combinations are supported in this release.

<table>
<thead>
<tr>
<th>Table 1-3 Supported Server Service Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
</tr>
<tr>
<td>Operations Manager</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Media Server(s)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Metadata Server</td>
</tr>
<tr>
<td>Maps Server</td>
</tr>
<tr>
<td>Federator</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Network (IP) and Analog Camera Support

Two types of cameras can be added to a Cisco VSM deployment:

- Network (IP) cameras—Network cameras are connect directly to the network and are added to Cisco VSM by entering the camera’s IP address and other settings.
- Analog cameras—Analog cameras are connected to an encoder. The encoder provides network connectivity and digitizes the analog video.

Both Cisco and third-party camera models are supported in a Cisco VSM deployment.

- Cisco cameras—Cisco offers a wide range of video surveillance cameras designed to take full advantage of Cisco VSM features and related Cisco technologies. See Cisco Video Surveillance IP Cameras for more information about the supported cameras and features.
- Third-party cameras—A wide range of third party cameras are also supported.
- See the Release Notes for your Cisco VSM release for a complete listing of the supported camera models, including firmware and other requirements.

Video Viewing Options

Live and recorded Cisco Video Surveillance video can be viewed using a Cisco-provided application, as summarized in Table 1-4.

Table 1-4 Summary of Cisco Video Viewing Options

<table>
<thead>
<tr>
<th>Viewing Tool</th>
<th>Application</th>
<th>Description</th>
<th>Documentation</th>
</tr>
</thead>
</table>
| Desktop monitoring application | Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) | Cisco SASD
  - Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation.
  - Create Video Matrix windows for display in separate monitors.
  - View Video Walls.
  - Create unattended workstations.
  - View and manage alerts.
  - View cameras, video, and alerts based on a graphical map. | Cisco Video Surveillance Safety and Security Desktop User Guide |
| Mobile device | Cisco VSM Mobile Viewer | Allows access to surveillance cameras using a phone or tablet to remotely monitor live streams and recorded video streams. | See the following for more information:
  - Apple iTunes—Cisco VSM Viewer for iPhone and iPad.
### Table 1-4  Summary of Cisco Video Viewing Options (continued)

<table>
<thead>
<tr>
<th>Viewing Tool</th>
<th>Application</th>
<th>Description</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based configuration and monitoring tools</td>
<td>Operations Manager Federator</td>
<td><strong>Operations Manager</strong>&lt;br&gt;- Allows simultaneous viewing of multiple video panes:&lt;br&gt;- View up to 4 cameras with the 32-bit version of Internet Explorer.&lt;br&gt;- View up to 25 cameras with the 64-bit version of Internet Explorer.&lt;br&gt;- Create the Views and Video Walls available in the desktop Cisco SASD application.&lt;br&gt;- Configure the camera, streams and recording schedules.&lt;br&gt;<strong>Cisco VSM Federator</strong>&lt;br&gt;- Cisco VSM Federator</td>
<td>Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
<tr>
<td>Desktop video clip player</td>
<td>Cisco Video Surveillance Review Player (Cisco Review Player)</td>
<td>Simple player used to view video clip files.</td>
<td>Cisco Video Surveillance Review Player</td>
</tr>
<tr>
<td>Web-based server console</td>
<td>Cisco Video Surveillance Management Console (Cisco VSM Management Console)</td>
<td>Provides basic viewing features for a single stream (Stream A) from a single camera.</td>
<td>Cisco Video Surveillance Management Console Administration Guide</td>
</tr>
</tbody>
</table>

**Note**

Video is recorded at GMT, but displayed in local time (the time where the user is viewing the video). For example, if a user is viewing EST video from a PST time zone, the video will display the PST time. See [Understanding NTP Configuration, page 9-1](#) for more information.
Monitoring Hardware Requirements

Cisco VSM video can be viewed from a variety of devices, including the PCs, mobile devices, and unattended monitors. Table 1-5 summarizes the requirements for each type of device.

<table>
<thead>
<tr>
<th>Monitoring Device</th>
<th>Description</th>
<th>Requirements and Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC computer</td>
<td>A PC workstation is used to monitor Cisco VSM video using one or more of the following:</td>
<td>Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</td>
</tr>
<tr>
<td></td>
<td>• Web browser monitoring</td>
<td>Refer to Using the Cisco Video Surveillance Monitoring Workstation Profiler Tool to analyze the ability of a PC client to render video.</td>
</tr>
<tr>
<td></td>
<td>– Cisco VSM Operations Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Cisco VSM Federator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Cisco VSM Management Console</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Desktop applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Cisco SASD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Cisco Review Player</td>
<td></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>The Cisco VSM Viewer app can be installed on an iOS (Apple) or Android mobile device.</td>
<td>See the following for more information:</td>
</tr>
<tr>
<td>Unattended Video Wall display</td>
<td>An unattended workstation is a PC that is used to monitor Video Walls without user input or interaction. Unattended workstations can be operated without a mouse or keyboard, and require the same specifications as a monitored workstation.</td>
<td>Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to Using the Cisco Video Surveillance Monitoring Workstation Profiler Tool to analyze the ability of a PC client to render video.</td>
</tr>
</tbody>
</table>
PART 2

Best Practices
Best Practices

Review the following best practices before deploying Cisco Video Surveillance Manager (Cisco VSM) to ensure your network, devices, and system is ready to successfully capture, record and display video.

- General Best Practices Guidelines, page 2-1
- Document Your System Before You Begin, page 2-3
- Network Links, page 2-5
- Network Reachability, page 2-5
- Dual-Stream and Custom Configurations, page 2-5
- VSM 7 Audio Support, page 2-6

General Best Practices Guidelines

Table 2-1 presents a list of best practices that have been established through a combination of design experience, scalability and performance evaluation, and internal Cisco trials.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Best Practices Guidelines</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation performance and requirements</td>
<td>Verify that monitoring workstation meet the baseline specification requirements. You can also use the Profiler Tool to analyze hardware performance.</td>
<td>- Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification</td>
</tr>
<tr>
<td>Supported Devices</td>
<td>Verify that the cameras and encoders in your deployment are supported by the Cisco VSM release.</td>
<td>Release Notes for Cisco Video Surveillance Manager</td>
</tr>
<tr>
<td>Network (NAT) reachability</td>
<td>Cameras and Cisco Media Servers can be installed within a single network (NAT) or in multiple NATs. Devices installed in different networks must be configured with the correct IP addresses to provide network communication.</td>
<td>Adding Cameras From Different Networks (NATs), page 8-11</td>
</tr>
<tr>
<td>Network port access</td>
<td>Cisco VSM release 7 servers must be able to receive network traffic from other VSM servers, cameras and user workstations on specific network ports.</td>
<td>Network Port Requirements, page 8-3</td>
</tr>
</tbody>
</table>
In the default and recommended NTP configuration, the Operations Manager is configured with an NTP server, and all other servers, cameras and encoders use the Operations Manager as their NTP server. This ensures that all devices, recordings, timestamps, alerts, and other resources are synchronized. Additional options are available, if required by your deployment.

Note Video is recorded at GMT, but displayed in local time (the time where the user is viewing the video). For example, if a user is viewing EST video from a PST time zone, the video will display the PST time.

DNS servers

We recommend configuring all Cisco VSM servers in DNS.

- Up to three DNS servers can be configured.
- Co-located VSOM/Media Servers must be in DNS to allow users to stream video from that server.

DHCP server

A DHCP server can be used to automatically assign the IP address, default gateway and DNS server for an Ethernet port.

Backup power supply

Install a backup power supply for all servers to protect against data loss and corruption if power is unexpectedly lost.

Data and video backups

Backup all server data to a remote source such as a FTP/SFTP site and/or tape backup. This allows your data to be recovered, or a server to be restored, if necessary.

Graphics cards and workstation performance

Use the supported graphics cards and specification for all PCs used to monitor video.

Camera stream settings

Cisco VSM release 7.x provides High, Medium, and Low video quality settings for supported devices. These settings have been tested and, unless otherwise noted, work in single stream mode and in all combinations in dual stream mode.

System and device software

Verify that the server and device software is up to date.

- Release Notes for Cisco Video Surveillance Manager
- Cisco Video Surveillance Manager: Install and Upgrade Guide

Security

Review the security best practices to secure your video data and system integrity.

Understanding NTP Configuration, page 9-1

DNS Server Support, page 8-7

Using Dynamic Host Configuration Protocol (DHCP), page 8-6

Cisco Video Surveillance Operations Manager User Guide

Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification

Dual-Stream and Custom Configurations, page 2-5

Securing Cisco Video Surveillance Manager, page 3-1
Document Your System Before You Begin

Before you begin, document all of the cameras, servers, IP addresses, serial numbers, device names, locations, network connections and other details for your deployment. Use a spreadsheet or other means to keep track of the devices, settings and configurations in your deployment. Update this document as it changes.

Tip

The more information you organize and document up front, the easier your deployment and on-going support will be.

The following table lists some, but not all, of the information you should document.

Table 2-2 Documentation Best Practices

<table>
<thead>
<tr>
<th>Resource/Topic</th>
<th>Documentation</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network topology</td>
<td>Prepare a high-level network topology diagram that displays the place of VSMS, and VSOM servers in the network, network link speeds, and network connectivity between various sites.</td>
<td>☐</td>
</tr>
<tr>
<td>Serial Numbers</td>
<td>Note the serial numbers for the servers, cameras, and encoders.</td>
<td>☐</td>
</tr>
</tbody>
</table>
Device configuration data

Document and use the following configuration details for each Cisco Media Server, video camera, and encoder:

- IP address
- NTP server
- Hostname
- Serial number
- Domain Name System (DNS) name
- Login credentials:
  - Cisco Media Servers—Management Console (VSMC) password
  - Cameras/encoders—device username and password
- Domain name
- Time zone
- Cameras/encoders—Cisco Media Server that will manage the device

Naming conventions

Consult with the customer about creating naming conventions for servers, cameras, encoders, views, template names, and user roles and user groups.

Video Stream configurations

- Document expected feed configurations for all cameras: camera type, resolution, media type, and frame/bit rate, and so on.
- Discuss with the customer expected video stream configurations. In a lab environment, configure the camera video streams in Cisco VSM Operations Manager and show the video to the customer.

  Note
  Changes in the feed configuration affect the actual video and disk space utilization.

Video archives (recordings)

Document configurations all archives: type of archives, duration, expiration, and so on.

Basic use cases

Identify basic use cases for a configuration:

- Use of archives (duration)
- Users, roles, and permissions
- Motion detection events
- Schedules
- Device triggers, soft triggers
- Backups
- Views (static vs. rotating)
Network Links

Table 2-3  Network Links: Best Practices

<table>
<thead>
<tr>
<th>Resource/Topic</th>
<th>Best Practice</th>
<th>Complete (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server and client links</td>
<td>The Cisco Media Servers, Operations Manager server, and Cisco VSM client workstations are connected to a 1 Gb full-duplex, network link. Verify the link speed and duplexity from each switch, server, or client workstation.</td>
<td>☐</td>
</tr>
<tr>
<td>Camera/encoder links</td>
<td>The IP cameras and encoders are connected to a 100-Mbps full-duplex link.</td>
<td>☐</td>
</tr>
<tr>
<td>Cable distance</td>
<td>The cable distance between switch port and servers, client workstations, IP cameras, or encoders is within the maximum allowed distance for the link speed and cable type.</td>
<td>☐</td>
</tr>
<tr>
<td>Switch ports</td>
<td>The IP cameras, encoders, servers, and client workstations are connected to individual switch ports; they are not connected to a hub.</td>
<td>☐</td>
</tr>
</tbody>
</table>

Network Reachability

Table 2-4  Network Reachability: Best Practices

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Complete (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP cameras, encoders, servers, client workstations are reachable on the network.</td>
<td>☐</td>
</tr>
<tr>
<td>The VSMS servers are reachable from the VSOM server, as well as client workstations using both hostname and IP address.</td>
<td>☐</td>
</tr>
<tr>
<td>The VSOM server is reachable from the VSMS servers using a hostname and IP address.</td>
<td>☐</td>
</tr>
</tbody>
</table>

Dual-Stream and Custom Configurations

This release provides validated High, Medium, and Low video quality settings for video supported devices. These settings have been tested and, unless otherwise noted, work in single stream mode and in all combinations in dual stream mode.

Custom settings allow customizing video settings for both single and stream and dual stream situations. The single stream custom settings are validated to allow only what a device supports. However, in dual-stream situations with custom settings, VSM 7 does not validate that the device supports a configured dual stream custom combination. The device may reject the configuration VSM may report
an error to the user. In some cases, the device may accept the configuration but deliver poor quality video or video at a different frame rate or bit rate than what was requested. When using custom settings, make sure to verify that the video quality is acceptable after configuring the camera.

**VSM 7 Audio Support**

This section describes HOW to configure the audio features in VSM 7 and how to use it with various endpoints.

**Legality of recording**

The laws regarding the recording of other persons and property by means of video recording and audio recording vary by location. In many places, it is common for the recording of public property, persons within the public domain, and of private property visible or audible from the public domain to be legal. But laws have been passed in many places restricting such activity in order to protect the privacy of others. Audio recording without consent can consequence in criminal charges or civil suits. So, if you're thinking about audio recording in a room to record conversations, you'll need to take a look at the applicable laws.

**Prerequisites**

To record audio on VSM:

- The cameras must support audio and be enabled. Audio is disabled in many cameras by default. Use the camera UI to enable Audio on the device.
- The audio icon will not display if your workstation monitor is set to 16-bit color setting. Change your monitor color setting to 32-bit.

**Configuring Live and Recorded Audio**

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enable audio in the camera template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Log in to the Operations Manager.</td>
</tr>
<tr>
<td>b.</td>
<td>Select <strong>Cameras &gt; Templates</strong> and select a template.</td>
</tr>
<tr>
<td>c.</td>
<td>Select a “<strong>Record Audio</strong>” setting (in the <strong>Streaming, Recording and Events</strong> tab).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Off</strong>—(Default) Audio is disabled for both live and recorded video playback.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Live Only</strong>—Audio is enabled for live video streaming only.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Live and Recorded</strong>—Audio is enabled for live streaming and recorded video playback.</td>
</tr>
</tbody>
</table>

⚠️ **Note**

The audio settings is disabled if audio is not supported by the camera.
Step 2  Audio configuration settings should be checked and adjusted if necessary in the IP Camera or Encoder Web GUI. This is where the proper audio signal level must be set and the choice of an internal or external microphone can be made. Some cameras will automatically use an internal microphone if no external microphone is connected. If the signal level is set too low, audio will not be received by VSM and if it is set too high, it will be distorted and may not be useable.

Step 3  Once the template is applied to a camera, the Cisco VSM monitoring panes display an audio icon if the camera supports audio. Click the icon to enable or mute live audio volume. This control does not affect recorded video.

Other audio playback settings are available in the VSM Video Client. Video Clips can be created in MP4/MPX or CVA/CVX formats. Video clips created in MP4 format support Audio playback. But Video clips saved in CVA or CVX format do not support Audio playback.

See the Cisco Video Surveillance Operations Manager User Guide for more details including how to use audio when creating video clips.

External Microphone Suppliers and Examples

To use audio with VSM 7, a camera must have an audio input. IP Cameras and Encoders have inputs for external microphones and some IP cameras have built-in microphones. For best performance and audio quality it is highly recommended that an external microphone be used that is designed for surveillance applications. These microphones are designed to pick up sound over large areas and have accessories including external power supplies and external amplifiers to provide the proper signal levels into an IP camera or encoder. In some audio surveillance applications, an external audio processing unit called a “Compressor/Limiter” or “Compander” is used. It amplifies very soft sounds while limiting the loudness of very loud sounds to provide a better range of usable sound without distortion. Here are few companies that provide microphones and accessories for surveillance applications:

- ETS Microphones
- LOUROE Electronics
- Crown PZM-11

Signal Levels from External Microphones

External microphones will typically come in two forms – unamplified or amplified. Unamplified microphones provide a low signal level called “Microphone Level”, but they do not need any external power. Amplified Microphones require external power, and provide higher signal levels called “Line Level”. Sometimes and external amplifier is used with an unamplified microphone and this external amplifier provides Line Level signal output. Some microphone external amplifiers provide additional audio processing features such as the “Compressor/Limiter” or “Compander” functions mentioned above. It is important to make sure that the signal level of the output of a microphone or microphone amplifier matches the expected signal level of the input of an IP camera or encoder. If it does not, the audio may not be audible or it may be badly distorted.
Some external amplifiers also allow the signal level of the output to be changed between Microphone and Line Levels and also to fine tune the signal level. Here is a list of the devices that support audio with VSM 7 and their input signal levels that are supported:

<table>
<thead>
<tr>
<th>Cameras</th>
<th>Physical Connector (3.5mm or RCA)</th>
<th>Signal Levels for audio input</th>
<th>GUI support for adjusting input levels (supports CMAPI)</th>
<th>Built in Microphone</th>
<th>Audio type</th>
<th>Audio Compression</th>
</tr>
</thead>
<tbody>
<tr>
<td>2600</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>Yes</td>
<td>Two-way (full- and half-duplex), one-way, or audio off</td>
<td>G.711 A-Law, G.711 U-Law, G.726</td>
</tr>
<tr>
<td>2611/2620/2630</td>
<td>3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>No</td>
<td>Two-way (full- and half-duplex), one-way, or audio off</td>
<td>G.711 A-Law, G.711 U-Law, G.726</td>
</tr>
<tr>
<td>4300,4500,4300E,4500E</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>Yes</td>
<td>Two-way (full-duplex), audio off</td>
<td>AAC (encoding only), G.711 A-Law, G.711 U-Law</td>
</tr>
<tr>
<td>6000P</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>Yes</td>
<td>Two-way (full-duplex), audio off</td>
<td>G.711 A-Law, G.711 U-Law</td>
</tr>
<tr>
<td>6020, 6030, 6400</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>No</td>
<td>Two-way (full-duplex), audio off</td>
<td>G.711 A-Law, G.711 U-Law</td>
</tr>
<tr>
<td>7030</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>No</td>
<td>Two-way (full-duplex), audio off</td>
<td>G.711 A-Law, G.711 U-Law</td>
</tr>
<tr>
<td>3520, 3530</td>
<td>1,3.5-mm Audio Jack</td>
<td>Line Level</td>
<td>Yes</td>
<td>No</td>
<td>Two-way (full-duplex), audio off</td>
<td>G.711 A-Law, G.711 U-Law</td>
</tr>
<tr>
<td>3421V</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
Securing Cisco Video Surveillance Manager

This document provides best practices and recommendations to ensure the security of Cisco Video Surveillance (Cisco VSM) components, including the Cisco VSM Operations Manager, Cisco Media Servers, Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application, video devices, and client PCs.

A video surveillance system typically captures valuable, confidential, and sensitive information. This information also is often required for command and control, and for critical decisions. It is important that you secure your video surveillance deployment to protect your information, thwart bad actors and disruptive actions, and prevent accidental or intentional destruction of data.

By following the guidelines in this document, you can help to protect your video surveillance system against physical threats and unauthorized access or configuration changes. You can also establish audit trails to assist with resolution if issues do occur.

Note

These guidelines are one part of a comprehensive approach to deploying a secure system. They should be considered in addition to other security and protective measures that you have established for your organization and video surveillance network.

Contents

This document includes the following sections:

- Controlling Physical Access, page 3-2
- Establishing a Secure Network Topology, page 3-2
- Changing Default Passwords, page 3-2
- Session and Password Timeouts, page 3-3
- Configuring Port Access for Cisco VSM, page 3-4
- Using Secure Remote Access, page 3-4
- Configuring User Roles and Access, page 3-4
- Administration and Monitoring Tools, page 3-5
- Logging Out from Management Console and Operations Manager, page 3-5
- Securing Client Systems, page 3-5
Controlling Physical Access

It is important to prevent unauthorized physical access to hardware components in a video surveillance network. Such access could lead to disruption of your live video or recording operation by someone disconnecting or powering down a component. It could also lead to loss of data by someone removing a video storage device.

To control physical access to video surveillance components, consider the following guidelines:

- If possible, place components in areas where you can control who can access the areas. For example, consider placing servers in locked cages or rooms.
- Lock components in racks.
- Lock cameras in their locations or use vandal-resistant devices.
- Protect network cables and other infrastructure components.

Establishing a Secure Network Topology

A secure network topology helps prevent the risk of unauthorized access to your video data and helps to prevent malicious network attacks.

To establish a secure network topology, deploy Cisco VSM software, clients, servers, and video devices in the same secure network, which is a network that is physically or logically separated from general access networks.

If necessary, you can allow clients from outside the network access to Cisco VSM servers. However, it is a best practice to use standard network methodologies to limit or control such access to the maximum extent possible.

In addition, it is a best practice to isolate video devices from general users and viewers on a network. To do so, follow these guidelines:

- Create one or more separate VLANs for video devices. Make sure that each VLAN limits access to monitoring and administrative users only.
- On network switches, configure access lists to allow Cisco Media Servers to access these VLANs.

Changing Default Passwords

Before you begin to operate a VSM system, change all default passwords. Use passwords that are not easy to guess, and control who has access to the passwords. A strong password prevents someone who knows a default password from accessing your system.

Passwords to change include the following:

- Cisco VSM Management Console password
- Operations Manager “admin” Password
- Camera and Encoder passwords
Session and Password Timeouts

In the Operations Manager, set the session timeout to the shortest period that is appropriate for your operation. This approach helps reduce the risk of unauthorized access unattended systems. Also define the password and username rules to help ensure users use a strong password.

Procedure

**Step 1** Log in the Operations Manager.

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

**Step 3** In the **General** settings, define the **User Timeout**:
- Enter the number of minutes before a user is automatically logged out due to inactivity. After this period, users must reenter their username and password to log back in.
- The maximum value is 10080 minutes (168 hours / 7 days).

**Step 4** In addition, define the password settings to ensure password security:

**Table 3-1 Password Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiry Months</td>
<td>The number of months before a user password automatically expires. At the end of this period, users are required to enter a new password.</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>The minimum number of characters for a valid password. Passwords with less characters than the entered value are rejected.</td>
</tr>
<tr>
<td>Maximum Password Length</td>
<td>The maximum number of characters for a valid password. Passwords with more characters than the entered value are rejected.</td>
</tr>
<tr>
<td>Identical Password/Username Allowed</td>
<td>If selected, user passwords can be the same as their username. If de-selected, user passwords must be different than their username.</td>
</tr>
<tr>
<td>3 Password Groups Required</td>
<td>If selected, user passwords must include characters from at least three different types of characters, including: lower case letters, upper case letters, symbols, numbers. If de-selected, user passwords can include only one type of character (for example, all lower case letters).</td>
</tr>
<tr>
<td>Repeat Characters</td>
<td>If selected, user passwords can repeat the same 3 characters. If de-selected, user passwords can not repeat the same 3 characters.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Save**.
Configuring Port Access for Cisco VSM

Cisco VSM servers include a firewall that is configured to allow services that might be needed for Cisco VSM applications to pass through. As a best practice, open only ports in the firewall that are required for your Cisco VSM deployment. This approach prevents the risk of disruption to your system through unauthorized access to services that your system runs.

See Network Port Requirements, page 8-3 for a summary of the ports required for Cisco VSM 7 servers to receive network traffic from other Cisco VSM servers, cameras and user workstations.

Using Secure Remote Access

Network communication between the browser (client) and the Operations Manager or the Management Console is encrypted using SSL and HTTPS. Each server includes a default self-signed SSL certificate, or you can upload a custom .pem certificate file issued by a Certificate Authority.

The self-signed or custom certificate is also used for back-end communication between Cisco Video Surveillance components, such as between the Operations Manager, Media Server and/or Management Console.

To create and install the SSL certificate, see the “Security” instructions in the Cisco Video Surveillance Management Console Administration Guide.

Configuring User Roles and Access

As a best practice, create users that have access to the locations, cameras, and video that they require. Cisco VSM users can monitor video or configure the system based on the following:

- The user group(s) to which the user is assigned: user groups are associates with a user Role, which defines the access permissions for the group.
- The location assigned to the user group(s).
- Users can be assigned to multiple user groups, and gain the combined access permissions for all groups.

Before you begin, carefully review the Cisco Video Surveillance Operations Manager User Guide for instructions to define the Locations, User Roles and User Groups. See this document to create the users that are assigned to these attributes.

User accounts provide access to both the browser-based Operations Manager and the Cisco Safety and Security desktop application.
Administration and Monitoring Tools

Live and recorded Cisco Video Surveillance video can be viewed using a Cisco-provided application, or a third-party application that supports Cisco VSM controls. See Video Viewing Options, page 1-8 for a summary of the available Cisco-provided options.

Note

Linux root user access and functions are not supported.

Logging Out from Management Console and Operations Manager

As a best practice, always log out and close the browser when you leave a Cisco VSM session. Logging out and closing the browser or application helps reduce the risk of unauthorized access to unattended systems.

Securing Client Systems

On each client system in a video surveillance network, follow these guidelines:

- Make sure that the current Microsoft Windows update is installed. These updates typically provide increased security features.
- Make sure that an industry-standard anti-virus program is running.
PART 3

Deployment Considerations
Deployment Scenarios

The fundamental factor when designing a Cisco VSM deployment is determining where the Cisco Video Surveillance Manager (Cisco VSM) servers will be located. This determination is based on the bandwidth requirements of your surveillance video, and the performance of your network.

This document provides a high-level overview of typical deployment scenarios.

- **Overview**, page 4-2
- **Deployment Scenarios, page** 4-3
  - Scenario 1: Centralized Data Center Architecture, page 4-3
  - Scenario 2: Centralized Management, Distributed Architecture, page 4-4
  - Scenario 3: Distributed Management, Distributed Architecture, page 4-5
- **Additional Deployment Scenarios and Options, page** 4-6

**Additional Information**

- Deployment Summary Steps, page 5-1
- Determining the Required Resources, page 6-1
Overview

A Cisco Video Surveillance Manager deployment starts with the location of your video cameras and the servers that support them. Specifically, you must determine where the Cisco VSM Operations Manager server and Cisco Media Servers will be located.

This chapter describes the basic server deployment scenarios, including the following:

- **Scenario 1: Centralized Data Center Architecture, page 4-3**—In the simplest deployment, all Cisco VSM servers are located in a central location, such as a rack in a network operations center (NOC). Cameras at various buildings or sites send all video traffic to the NOC servers. This scenario can be used if you have only a few cameras at each site, or plentiful network bandwidth.

- **Scenario 2: Centralized Management, Distributed Architecture, page 4-4**—In this scenario, Cisco Media Servers are deployed in the same location (LAN) as the cameras. This can be used if you have cameras at remote sites that generate large amounts of video traffic, or if the network connection to the remote site has limited or expensive bandwidth. Installing the Media Server(s) at the camera location reduces network traffic between the remote site and the NOC (since cameras continuously stream video to their Media Servers).

- **Scenario 3: Distributed Management, Distributed Architecture, page 4-5**—If multiple Operations Managers are deployed, you can install a Cisco Video Surveillance Federator (Federator) server to monitor video and events from all Operations Managers.

- **Additional Deployment Scenarios and Options, page 4-6**—A combination of deployment scenarios can be used depending on the network resources and bandwidth available of each location in your deployment.

See Determining the Required Resources, page 6-1 for a ways to reduce the bandwidth between cameras and the Cisco Media Servers.
Deployment Scenarios

The scenarios described in this document are simplified for clarity. Your organization may use a mix of these scenarios, such as most servers deployed in a central location, some cameras in remote sites without an on-site Cisco Media Server, other sites with cameras and on-site Media Servers, and an additional site with limited bandwidth that uses Dynamic Proxy (DP) to minimize the network traffic from that location.

Review each of the following scenarios to understand the options for Cisco VSM server location.

- Scenario 1: Centralized Data Center Architecture, page 4-3
- Scenario 2: Centralized Management, Distributed Architecture, page 4-4
- Scenario 3: Distributed Management, Distributed Architecture, page 4-5
- Additional Deployment Scenarios and Options, page 4-6

Scenario 1: Centralized Data Center Architecture

In a centralized deployment (Figure 4-1), all Cisco VSM servers are located in a single network operations center (NOC) or rack. This includes the Operations Manager, Media Servers, and any optional Long Term Storage (LTS), Federator, Dynamic Proxy (DP), Metadata, or Maps servers. Servers can be installed as physical appliances, or as virtual machines (VMs) running on Cisco UCS blades.

The cameras for a centralized deployment can be installed in a multiple networks (NATs), and securely communicate with the central servers over a WAN or public Internet. Users who monitor the video can also be at different locations and networks.

Figure 4-1 Centralized Data Center Architecture
This scenario is typically used by school districts or businesses where cameras are at various locations but the server infrastructure is in a central administrative location.

Note: All servers can be installed as physical or virtual machines (VMs). VMs can run on a variety of supported Cisco UCS platforms. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Scenario 2: Centralized Management, Distributed Architecture

Video surveillance cameras continuously stream video to their associated Media Servers, even if video is not being recording or monitored. This provides on-demand video access to users, and for recordings if an event occurs.

This on-demand video requires sufficient bandwidth between the network where the cameras are installed and their associated Media Servers that manage and record that video. If network bandwidth is limited, slow, or expensive, performance, quality, or cost issues can occur.

To address these issues, a distributed deployment can be used (Figure 4-2). In this deployment architecture, the management servers (such as the Operations Manager, Long Term Storage, and Dynamic Proxy servers) are still located in a central NOC, but the Media Servers are installed in the networks where cameras and encoders are located. Since video is streamed from the cameras to the Media Servers, this distributed deployment greatly reduces the amount of video traffic sent between networks since video is only sent from the Media Server to users (or a Long Term Storage server) when requested.

In the Figure 4-2 example, the Operations Manager is centrally-located in a NOC, along with optional LTS storage servers and a Dynamic Proxy server. The Media Servers are installed in the same locations as the cameras and encoders they support.

Figure 4-2 Centralized Management, Distributed Architecture
Note

All servers can be installed as physical or virtual machines (VMs). VMs can run on a variety of supported Cisco UCS platforms. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Scenario 3: Distributed Management, Distributed Architecture

Some enterprises, such as school districts, install multiple Cisco VSM deployments, each with an independent Operations Manager server. In this scenario, a Cisco VSM Federator server can be installed to allow central office personnel to monitor video from all Cisco VSM deployments (Figure 4-3).

Figure 4-3  Cisco Video Surveillance Federator

The Cisco Video Surveillance Federator provides the following benefits:

- Easily connect and monitor up to 5 million cameras
- Provides for an operational integration for up to 500 VSOMs
- Single pane of glass to monitor live and archive video from all end points globally
- Configurable level of alerts to consolidate and display to Federator user
- Minimal configuration through use of regions and sites to represent VSOM systems

For example, a city-wide deployment may include a Cisco VSM system for each independent agency, such as the county court, schools, police, post office and fire department. Each of these deployments includes an Operations Manager server that is used to configure the cameras, users, and features for that agency or department.

To allow central employees or security personnel to monitor the video from all Cisco VSM deployments, a Cisco VSM Federator server is installed in a central location. The Federator provides video monitoring without giving them direct access to the administrative and configuration features.
All servers can be installed as physical or virtual machines (VMs). VMs can run on a variety of supported Cisco UCS platforms. See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

**Additional Deployment Scenarios and Options**

Each of the deployment scenarios described in this document can be combined with other server and storage options, such as on-camera recording (Connected Edge Storage), Dynamic Proxy, high availability, long term storage, Maps server, Metadata servers, and other features. Use of these options depend on the on your organization’s need and the network resources available from the various locations in your deployment. Table 4-1 summarizes some of the features and options that can be combined with any of the main deployment scenarios described in this document.

**Figure 4-4 Combining Scenarios in a Sample Deployment**

**Table 4-1 Hybrid Deployment Scenarios**

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized NOC</td>
<td>Most Cisco VSM servers may be located in a central operations center.</td>
<td>Scenario 1: Centralized Data Center Architecture, page 4-3</td>
</tr>
<tr>
<td>High-bandwidth location</td>
<td>Cameras are installed at another location, and communicate directly with the Cisco Media Servers in the Centralized NOC. Network bandwidth and cost are sufficient for the amount of video traffic from the cameras at that site.</td>
<td>Scenario 1: Centralized Data Center Architecture, page 4-3</td>
</tr>
</tbody>
</table>
### Additional Deployment Scenarios and Options

**Limited bandwidth location**

Cisco Media Servers are installed in the same location as the cameras. This reduces the amount of video traffic from the remote site to the central NOC since the cameras communicate video traffic directly to the on-site Media Servers.

This scenario is used for locations where bandwidth is limited or expensive based on the amount of video traffic generated by the cameras at that site. This greatly reduces the amount of network traffic between different NATs.

**Scenario 2: Centralized Management, Distributed Architecture, page 4-4**

**Low-bandwidth locations**

For sites that have very limited, expensive, or low bandwidth, Dynamic Proxy can be configured to minimize video traffic from that site.

**Using Dynamic Proxy to Monitor Video From Low-Bandwidth Sites, page 11-1**

**On-camera recording**

For sites when recording is only required on demand, or when cameras are off the network for periods of time.

**On-Camera Recording (Connected Edge Storage), page 7-3**

**Multiple Cisco VSM deployments**

Use Cisco Video Surveillance Federator to monitor video and events from multiple independent deployments (such as Figure 4-4).

**Scenario 3: Distributed Management, Distributed Architecture, page 4-5**

**Server high availability (HA)**

- Multiple Cisco Media Servers can be installed to provide redundant video recording or failover capability if the primary server goes down.
- Media Servers can be deployed as Long Term Storage (LTS) servers to allow video archives to be archived on a separate server.
- Two Operations Manager servers can be deployed to provide failover capability if the primary server goes down.
- Cisco VSM can be deployed in virtualized environment on a UCS B- and C-Series servers using VMware HA.

**Server High Availability, page 12-1**

---

### Table 4-1  Hybrid Deployment Scenarios (continued)

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Description</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited bandwidth location</td>
<td>Cisco Media Servers are installed in the same location as the cameras. This reduces the amount of video traffic from the remote site to the central NOC since the cameras communicate video traffic directly to the on-site Media Servers. This scenario is used for locations where bandwidth is limited or expensive based on the amount of video traffic generated by the cameras at that site. This greatly reduces the amount of network traffic between different NATs.</td>
<td>Scenario 2: Centralized Management, Distributed Architecture, page 4-4</td>
</tr>
<tr>
<td>Low-bandwidth locations</td>
<td>For sites that have very limited, expensive, or low bandwidth, Dynamic Proxy can be configured to minimize video traffic from that site.</td>
<td>Using Dynamic Proxy to Monitor Video From Low-Bandwidth Sites, page 11-1</td>
</tr>
<tr>
<td>On-camera recording</td>
<td>For sites when recording is only required on demand, or when cameras are off the network for periods of time.</td>
<td>On-Camera Recording (Connected Edge Storage), page 7-3</td>
</tr>
<tr>
<td>Multiple Cisco VSM deployments</td>
<td>Use Cisco Video Surveillance Federator to monitor video and events from multiple independent deployments (such as Figure 4-4).</td>
<td>Scenario 3: Distributed Management, Distributed Architecture, page 4-5</td>
</tr>
<tr>
<td>Server high availability (HA)</td>
<td>- Multiple Cisco Media Servers can be installed to provide redundant video recording or failover capability if the primary server goes down.</td>
<td>Server High Availability, page 12-1</td>
</tr>
<tr>
<td></td>
<td>- Media Servers can be deployed as Long Term Storage (LTS) servers to allow video archives to be archived on a separate server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Two Operations Manager servers can be deployed to provide failover capability if the primary server goes down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Cisco VSM can be deployed in virtualized environment on a UCS B- and C-Series servers using VMware HA.</td>
<td></td>
</tr>
</tbody>
</table>
Deployment Summary Steps

Create a design plan that includes the following elements. Your plan should include network (NAT) boundaries and other network requirements, camera and encoder locations, and user access requirements. In addition, detail the Cisco VSM features required by your users, and the Cisco VSM servers and server services required to support those features.

Summary Procedure

The following steps provide a high-level summary of the process used to design a Cisco VSM deployment. Refer to the additional documentation for more information.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Design the network Review the network requirements and consideration for a successful Cisco VSM deployment. Your network’s performance, features, bandwidth, and other conditions, help define the deployment scenario(s) used by your organization. For example, the performance and policies for transmitting video traffic across network segments determines where servers are located, such as in a central NOC, in the same network segment as the cameras. Dynamic Proxy (DP) can be used for low-bandwidth locations. Additional considerations include quality-of-service (QoS) policies, remote sites connected with a low-bandwidth line, and bandwidth availability and cost.</td>
<td>Cisco Video Surveillance Solution Reference Network Design Guide—defines the network requirements, conditions, and bandwidth required for a Cisco Video Surveillance deployment.</td>
</tr>
</tbody>
</table>
### Task 2
**Determine the camera bandwidth requirements**

Determine the bandwidth required for the cameras in your deployment.

**Tip**
Most cameras stream video continuously to the Media Server. The camera bandwidth requirements are based on this and determine the number of Media Servers required to support those cameras, and the amount of network bandwidth required to transmit the video streams to the Media Servers.

Camera bandwidth requirements are calculated by multiplying the number of streams configured on each camera and the megabits (Mb) required for each stream.

**constant bit rate (cbr)**

For example, if 100 cameras each require 2 Mb of bandwidth to continuously stream video, then you will need:

- Enough Media Server capacity
- Sufficient bandwidth between the camera and the Media Servers.

### Task 3
**Determine the camera storage requirements**

Determine the amount of disk storage required for the camera recording and retention needs of your deployment.

You can add the following based on these needs:

- Additional Media Servers
- External storage arrays
- Long term storage (LTS) server(s)

### Task 4
**Determine the number of Media Servers**

Using the camera requirements from Task 2, determine the number of physical or virtual Media Servers required in your deployment.

**Note**
Use the Performance Guidelines to determine the maximum number of cameras supported by each server, and the maximum storage supported by those servers.
**Step 5**

Determine your deployment scenario(s)

Determine where the servers will be installed based on the sample deployment scenarios. Install the servers where the bandwidth is available: either at a central location or at each site where the cameras are installed.

For example, if the Media Servers are at a different site (LAN) than the NOC, then the video traffic will go over the Internet or Intranet. If that bandwidth is expensive or not available, then you can install Media Servers in the same location (LAN) as the cameras.

**Additional Information**

- Deployment Scenarios, page 4-1

**Step 6**

Review and implement the Cisco VSM best practices.

Best practices are essential to ensure a successful deployment, smooth operation and user satisfaction. For example, we highly recommend installing a UPS backup power supply for all server and including an automatic backup plan to protect against data and video loss or corruption.

Securing your Cisco VSM deployment is also critical to protect the privacy and integrity of your video and data.

**Additional Information**

- Best Practices, page 2-1
- Securing Cisco Video Surveillance Manager, page 3-1

**Step 7**

Define the server and storage requirements for the cameras.

The number, and location, of Cisco Media Servers required in your deployment is determined by the following:

- The number of cameras installed at each site (LAN). This will also be used to define the IP addressing required by the device to communicate with the Media Server.
- The video bit rate used for each camera (to determine the amount of network bandwidth required by the camera).

**Additional Information**

- Cisco Video Surveillance Manager Release 7 Server Performance Guidelines—How many cameras you can add to a Media Server.
- Server and Camera Network Configuration, page 8-1

**Step 8**

Define the Cisco VSM servers required by your deployment and the physical location of those servers.

- A minimum of one Operations Manager and one Media Server is required to deploy the Cisco Video Surveillance Manager. These can be co-located on a single server, or deployed as stand-alone servers.
- Additional Media Servers can be installed depending on the number of camera streams, recordings, and bandwidth limitations of your site.
- Determine the number of servers required based on the number of cameras. This will help you define the number of servers and their placement
- Additional server services, such as the Maps and Metadata servers, may require additional servers.

**Additional Information**

- Deployment Scenarios, page 4-1
- Understanding Cisco VSM Servers and Server Services, page 1-5
- Cisco Video Surveillance Manager Release 7 Server Performance Guidelines
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| **Step 9** | Define the HA requirements for your installed servers | - The Cisco Video Surveillance Operations Manager can be deployed as an HA pair to ensure uninterrupted service if the primary server goes down.  
- Cisco Video Surveillance Media Servers can be configured in a high availability (HA) arrangement that allows a primary server to be paired with additional Failover, Redundant, or Long Term Storage Media Server. These HA servers provide the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.  
- Video Surveillance Manager (VSM) Release 7.x Operations Manager in a virtualized environment on a UCS B- and C-Series server using VMware HA. | Server High Availability, page 12-1 |
| **Step 10** | Define the network NAT boundaries for the cameras and servers. | The camera and server network configuration (such as IP addressing) varies depending on whether the cameras are on the same network (NAT) as the servers, or if they are installed in a different network (and must communicate across NAT boundaries). | Server and Camera Network Configuration, page 8-1 |
| **Step 11** | DHCP | Determine if DHCP will be used to provide network addresses to your cameras, and the Media Servers used in camera discovery. | Using Dynamic Host Configuration Protocol (DHCP), page 8-6 |
| **Step 12** | NTP | Define the NTP requirements for your deployment. In a centralized deployment, the Operations Manager can act as the NTP server for all Media Servers. The cameras and encoders then use the Media Server as their NTP server. | Understanding NTP Configuration, page 9-1 |
| **Step 13** | Define user access permissions | Determine user access to live and recorded video based on user roles and cameras locations. For example, users may have certain access permissions to view live video at a specific building or campus, while other users may be able to view video and configure features at all locations. | Controlling User Access Permissions, page 16-1 |
### Chapter 5  Deployment Summary Steps

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| **Step 14** | Adding cameras | Define how your cameras will be added to Cisco VSM. The options are:  
- Add each camera manually.  
- Import a list of cameras from a CSV file.  
- Automatically discover the cameras when they are added to the network. | Discovering Cameras on the Network, page 15-1 |
| **Step 15** | Configuring cameras | Understand how camera configurations can be applied in bulk using templates, pre-configured settings, or bulk actions. | Bulk Camera Configuration and Deployment, page 14-1 |
| **Step 16** | Determine the streaming and recording policies |  
- **Recording**—Define the recording policies for the cameras. For example, cameras can continuously record video, record only if a motion event or other event occurs, or both. Numerous types of events can also be used to trigger recordings. Recordings can also be saved on the camera (if the device supports on-camera storage).  
- **Storage Requirements**—The amount of disk storage required by each camera (based on the recording length and how long the recordings are retained).  
- **Maps**—Use the Maps feature to display the real-world location of cameras on a map and view a video preview for that location.  
- **Video Walls**—Use video walls to display multiple video frames (from multiple cameras) on a single screen. Video Walls can be displayed in unattended mode, so people can see the monitor but not access the PC or change the view. |  
- Video Recording Options, page 7-1  
- Displaying Alerts and Devices on a Map, page 22-1  
- Deploying Video Walls, page 20-1 |
| **Step 17** | Define event-triggered actions. | Numerous types of events, such as motion, contact closure, or camera tampering, can trigger actions to occur. Actions include a variety of options, such as recording video or sending a notification.  
Video analytics can also be used to determine motion and other events from recorded video. |  
- Using Events to Trigger Actions, page 18-1  
- Using Video Analytics for Post-Event Motion Detection, page 19-1  
- Deploying Video Walls, page 20-1 |
<p>| <strong>Step 18</strong> | Use camera apps for advanced analysis | Camera apps can be installed for a variety of advanced analysis, such as creating an event when glass breaks or a gunshot occurs. | Using Events to Trigger Actions, page 18-1 |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Define additional camera features</td>
<td>The camera features may require specific configuration planning, bandwidth, storage, and firmware requirements. For example, identify which cameras require features such as pan-tilt and zoom (PTZ), on-camera recording, camera apps, or other Cisco VSM features</td>
<td>Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
<tr>
<td>20</td>
<td>Install the servers, cameras, and encoders.</td>
<td>Physically install the devices according to your network plan.</td>
<td>Cisco Video Surveillance Manager: Install and Upgrade Guide</td>
</tr>
<tr>
<td>21</td>
<td>Install the PC monitoring stations.</td>
<td>Install PC monitoring that meet the processing, memory and graphics requirements for a Cisco VSM deployment.</td>
<td>Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
<tr>
<td>22</td>
<td>Configure the devices and features for your deployment.</td>
<td>Use the browser-based Operations Manager to configure the servers, cameras, encoders, and features for your Cisco VSM deployment.</td>
<td>Controlling User Access Permissions, page 16-1</td>
</tr>
<tr>
<td>23</td>
<td>Configure user access and permissions</td>
<td>Configure the user roles, groups and accounts, and create the locations for your users and devices.</td>
<td>Using Video Analytics for Post-Event Motion Detection, page 19-1 Displaying Alerts and Devices on a Map, page 22-1</td>
</tr>
<tr>
<td>25</td>
<td>Monitor live and recorded video.</td>
<td>Use the desktop Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application to monitor video. Use unattended Video Walls to display surveillance video on a screen without a PC. Use the Cisco VSM mobile apps to monitor video from a mobile device.</td>
<td>Cisco Video Surveillance Operations Manager Mobile App User Guide</td>
</tr>
</tbody>
</table>
Determining the Required Resources

A successful Cisco VSM deployment includes sufficient server processing, network bandwidth, and video storage to reliably transmit video to end users, archive video data, and manage system policies. Refer to the following topics to determine the devices, resources and deployment scenario required by your organization.

- Factors That Determine Your Server Deployment Scenario, page 6-1
- Determine Bandwidth and Storage Estimates for Media Servers and Cameras, page 6-3
- Using the Guided System Selling Tool, page 6-4
- Methods to Reduce Video Bandwidth Usage, page 6-6

Factors That Determine Your Server Deployment Scenario

A successful Cisco VSM deployment depends on the ability of your Cisco VSM servers to process, deliver, and store video data, and the network’s ability to transport that video data between cameras, servers, end users, and long term storage devices.

Table 6-1 summarizes the three main factors used to determine the number and location of Cisco VSM servers required by your deployment.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server performance</td>
<td>The number of cameras, amount of video data, and storage supported by each Cisco Media Server. Performance numbers vary depending on the server model and configuration, and factors such as if the device is a physical or virtual machine. Use the Cisco Guided System Selling Tool to help determine the correct resources for your deployment.</td>
<td>• Using the Guided System Selling Tool, page 6-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Video Surveillance Manager Server Performance Guidelines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Methods to Reduce Video Bandwidth Usage, page 6-6</td>
</tr>
</tbody>
</table>
### Table 6-1  Factors to Determine Server Deployment Scenario (continued)

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Server storage              | The amount of storage supported by, and installed in each server. This is the amount of video and other data that can be stored before automatic pruning occurs. Deployments with greater recording needs or longer video archive retention times will require greater amounts of storage space. You can also install external storage arrays to increase the available storage. | • Cisco Video Surveillance Manager Server Performance Guidelines  
• Server Storage, page 10-1                                                      |
| Sizing servers to upgrade storage later | When selecting a server for Media Servers with the intention to be able to increase the server’s internal storage later, it is recommended to select a server with ½ of maximum number of hard drives (e.g. 12) so that an equal number of hard drives can be added later. Adding internal storage will require configuring an additional RAID-5/RAID-6 array with the new hard drives to create a new RAID volume (LUN); adding an equal number of drives will allow for a roughly equal size storage volume for recording additional cameras, and maximize the additional storage capacity. Adding a new RAID-5/RAID-6 array with only a few hard drives (e.g. 2-4) is less efficient use of the additional capacity. For example, a CPS-UCS-2RU-K9 server with a (12) drive capacity could be deployed with (6) 4TB hard drives, and later add an additional (6) 4TB hard drives, for an approximately 16TB capacity initially, and later add approximately 16TB more. | • Cisco Video Surveillance Manager Server Performance Guidelines  
• Server Storage, page 10-1                                                      |
| Network conditions          | The network policies, performance, and bandwidth required to support your deployment. For example:  
• Cameras in locations that have unlimited or inexpensive bandwidth communication to the central network operations center (NOC) can use a centralized deployment.  
• Cameras in locations where bandwidth is limited or expensive can use a distributed server deployment, on-camera recording, or a Dynamic Proxy server. | • The Cisco Video Surveillance Solution Reference Network Design Guide describes the overall network requirements and considerations, and the video considerations, such as how compression, codecs, and stream quality affect the amount of required bandwidth.  
• Video Recording Options, page 7-1—streaming and recording policies can have a big affect on the amount of storage and video bandwidth required by your deployment.  
• Using the Guided System Selling Tool, page 6-4  
• Methods to Reduce Video Bandwidth Usage, page 6-6 |
Determine Bandwidth and Storage Estimates for Media Servers and Cameras

The network in a Cisco VSM deployment must be able to continuously stream video from the cameras to the Cisco Media Servers, and from the Media Servers to the monitoring workstations in your deployment. The bandwidth requirements for each Media Server includes all of the video streams configured for its cameras, the bandwidth of the video streams from the Media Servers to other applications and to monitoring workstations. Depending on the location of the cameras, Media Servers and monitoring workstations, different segments of the networks will also have different bandwidth requirements.

For example, if cameras are installed in different network segments (NATs) than the Media Servers, then the network must have sufficient bandwidth between those segments for the video streams from all cameras. The bandwidth requirement is the aggregate data rate for all cameras assigned to a server. You must include all camera streams from each camera, and the different bit rates for each stream. For example, if a camera has dual video streams, you must include both streams in your bandwidth requirement calculations.

See Understanding Cisco VSM Data Flow, page 1-4 to determine the network segments in your deployment and the path of network traffic from cameras to Media Servers.

Table 6-2 describes the main factors used to determine the bandwidth needs for your deployment.

<table>
<thead>
<tr>
<th>Resource/Topic</th>
<th>Task</th>
<th>Complete (✓)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera bandwidth</td>
<td>Calculate per-camera bandwidth estimates based on the expected video stream, media type, resolution, and frame/bit rate.</td>
<td>![ ]</td>
</tr>
<tr>
<td>Media Server bandwidth</td>
<td>Calculate bandwidth requirement estimates for each Media Server based on expected number of video streams to the Media Server.</td>
<td>![ ]</td>
</tr>
<tr>
<td>Storage requirements</td>
<td>Calculate storage requirement estimates per Media Server based on expected number of archives in the Media Server, their expected duration, and video stream information. Include 7-minute loop archives in motion detection event setups.</td>
<td>![ ]</td>
</tr>
</tbody>
</table>
| Recommended                | • Consider disk space requirements for clips stored on the server. Even if the clip duration is (for example, 15 seconds), it occupies 5 to 10 minutes worth of disk space.  
• Consider disk space requirements for archive backups.  
• Consider future expansion plans and disk space requirements for new feeds and archives. | ![ ]         |
| Cisco Media Server performance | Based on the bandwidth and storage estimates, determine if the Cisco Media Server hardware can handle the expected configuration. Consider future expansion plans, if any. | ![ ]         |
Using the Guided System Selling Tool

Use the Cisco Commerce Workspace “Guided System Selling” tool to determine the resources required by your deployment, the prices for those components, and to order the devices and resources.

The resources include the total number of cameras, the total camera bit rate (Mbps), the number of required physical or virtual servers, licenses, network switches, and other resources required in your deployment.

Procedure

**Step 1** Log in to the Cisco Commerce Workspace.

**Step 2** Under Solutions, click **Guided System Selling** (lower right).

**Step 3** Under Available Solutions, select **Connected Safety and Security** and then **Video Surveillance** (Figure 6-1).

**Figure 6-1** Guided System Selling Tool

![Guided System Selling Tool](image)
Step 4  Complete the on-screen forms to determine the cameras, servers, licenses, network switches, and other resources required in your deployment (Figure 6-2).

Figure 6-2  Guided System Selling Tool
Methods to Reduce Video Bandwidth Usage

If bandwidth is limited between the video cameras and supporting Media Server, use one or more of the following methods to reduce the bandwidth created by the video streams, or reduce the traffic sent between network segments.

Table 6-3 Methods to Reduce Bandwidth

<table>
<thead>
<tr>
<th>Method / Feature</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Reduce the video stream framerate | Reduce the video stream framerate by configuring a lower bit rate. Although this reduces the video quality, it also reduces the amount of data sent over the network and stored in the archives. To reduce the video framerate, use one or more of the following methods: • Select low or medium video quality for the camera template. • Create a custom template. • Use the Recording Options to reduce the recording framerate or record only one stream to save storage. | • Cisco Video Surveillance Operations Manager User Guide  
• Video Recording Options, page 7-1 |
| Position servers closer to the cameras | Install the physical or virtual Media Servers in the same network segment (LAN). Most cameras stream video continuously so that it is instantly available for viewing or recordings. Installing the cameras in the same LAN prevents that traffic from being sent between network segments, such as over the Internet, where bandwidth can be more limited or expensive. | Scenario 2: Centralized Management, Distributed Architecture, page 4-4 |
| Use Dynamic Proxy                | If a Media Server is located in a low-bandwidth location, Dynamic Proxy (DP) can be configured to minimize the bandwidth used when video is requested from other locations. | Using Dynamic Proxy to Monitor Video From Low-Bandwidth Sites, page 11-1 |
**Table 6-3  Methods to Reduce Bandwidth (continued)**

<table>
<thead>
<tr>
<th>Method / Feature</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Economical Streaming          | By default, video cameras continuously stream video over the network to the Media Server. This allows users to instantly access live video, and recordings to being immediately when an event occurs. Economical Streaming is a camera feature that delivers video only when requested by a user, or when an event occurs. When selected:  
  - Video playback will be delayed while the request is being processed.  
  - When Economical Streaming is enabled, motion event alerts and other Advanced Event processing is disabled since video is only sent when requested by a user.                                                                                                           |  
  + Cisco Video Surveillance  
    Operations Manager User Guide  
  + Video Recording Options, page 7-1 |
| Connected Edge Storage        | Video cameras can use this feature to save video on the camera’s storage device (such as an SD card). This can be used with Economical Streaming (above) to eliminate the need for a local Media Server, and send video over the network only when requested.  
  - For example, if a camera with on-device storage is installed in a remote sub-station, video can be streamed continuously to the camera’s SD card. That video is not sent across the network to the Media Server unless requested by a user.  
  - If the camera is mobile, such as a camera installed on a bus, video can be saved to the camera’s storage when the bus is in service, and transferred to the Media Server when the bus (and camera) are back in network range. |  
  + On-Camera Recording (Connected Edge Storage), page 7-3  
  + Cisco Video Surveillance  
    Operations Manager User Guide |
Video Recording Options

Video can be recorded using a variety of automatic methods, or manually triggered by a user. Refer to the following topics for more information:

- **Summary of Recording Options, page 7-1**
- **Best Practices for Recording on Motion, page 7-2**
- **On-Camera Recording (Connected Edge Storage), page 7-3**
  - Deployment Scenarios, page 7-3
  - Copy Options, page 7-6
  - Important Performance Considerations with Connected Edge Storage, page 7-6

## Summary of Recording Options

Video can be recorded continuously, when an event occurs, or be manually triggered by a user.

### Table 7-1 Recording Options

<table>
<thead>
<tr>
<th>Recording Type</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous recording, scheduled recordings, and/or motion event recordings.</td>
<td>The recordings can occur continuously in a loop (for example, the past 30 minutes), or according to a schedule (such as Monday-Friday, 8 a.m. to 11 a.m.). In either case, recording can occur for the entire time, or only when triggered by a motion event.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Configuring Continuous, Scheduled, and Motion Recordings</td>
</tr>
<tr>
<td>Video is recorded at different quality on Stream A and Stream B.</td>
<td>For example, you can record continuous video throughout the night at a lower quality, but also record higher-quality video whenever an event occurs. You can also merge the recordings from Stream A and Stream B into a single timeline.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Understanding (and Merging) Video Streams</td>
</tr>
<tr>
<td>Recording is triggered when an event occurs.</td>
<td>Recordings can be triggered when an event occurs. For example, recording can occur when a door contact is opened or closed, when a camera app event occurs, or when a soft trigger is received. You can define how long to record when the event occurs, and whether to record the primary or secondary stream.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Using Advanced Events to Trigger Actions</td>
</tr>
</tbody>
</table>
Best Practices for Recording on Motion

When using motion recording in Cisco VSM, there are several important considerations that should be followed to properly control the recording of video with motion detection.

Cisco VSM supports configuration for default motion detection settings to allow quick setup of camera motion detection. The motion detection inclusion window is set to the full frame and sensitivity is set to a default value. These settings may or may not be optimal for detecting video in all situations depending on many factors such as lighting, the camera placement and if there is extraneous motion in the scene. For example, if there is an area in the frame where there is always motion, the camera may continuously detect motion and motion recording will continuously record video. Prior to Cisco VSM 7.6, recording would stop by default after 2 hours of continuous motion activity. In Cisco VSM 7.6, that behavior has been changed and motion based recording will continue as long as there is motion activity. This may negatively affect video retention for all cameras on the same Media Server, if this motion recording behavior is not expected.

Review the following best practices and recommendations when using motion recording.

- Do not rely solely on the default motion detection settings for motion recording for outdoor cameras without assessing the results. Outdoor scenes are more complex with changes in lighting (day/night), clouds, people, cars, trees, and leaves moving in the wind. For outdoor cameras, it is very common to have extraneous motion that should be ignored because that activity is not of interest. First, adjust the zoom and focus so the camera’s field of view and focus so that the detection settings are optimal for all moving objects in that field of view. Second, the motion detection inclusion and/or exclusion windows should to be set, not just the sensitivity settings. This helps to accurately trigger recording for the important motion activity while ignoring undesired activity. Roads and trees in the background are common causes of unexpected motion activity where motion only in the foreground is desired for controlling recording.

- When configuring motion recording, make sure that the camera is detecting motion as expected. Use the Operation Manager’s motion detection configuration page to observe the camera’s motion activity, and ensure the field of view is correct. Make sure that motion is being detected as expected and adjust the inclusion and exclusion windows and settings as needed.

<table>
<thead>
<tr>
<th>Recording Type</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-initiated recording</td>
<td>Describes how to enable the On Demand Recording option when a user right-clicks a camera’s live image.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Enabling On Demand Recording</td>
</tr>
<tr>
<td>Save recordings on the camera (and optionally transfer them to the Cisco Media Server).</td>
<td>Cameras that support on-device storage of video recordings can be used to record video even if the camera does not have communication with the Cisco Video Surveillance system. Once network communication is re-established, the on-camera recordings can be copied to a Media Server.</td>
<td>• Cisco Video Surveillance Operations Manager User Guide &gt; Connected Edge Storage (On-Camera Recording) • On-Camera Recording (Connected Edge Storage), page 7-3</td>
</tr>
</tbody>
</table>

Table 7-1 Recording Options (continued)
When configuring motion detection for a camera using Operation Manager, always click the Save Motion Config button to save changes before closing the browser or leaving the motion configuration page. If you do not save the motion settings, the motion detection recording will not operate as intended.

On-Camera Recording (Connected Edge Storage)

Connected Edge Storage allows video recordings to be saved on the camera (typically an SD card installed in the camera). These recordings can be automatically or manually copied to the Cisco Media Server.

Refer to the following topics for more information:
- Deployment Scenarios, page 7-3
- Copy Options, page 7-6
- Important Performance Considerations with Connected Edge Storage, page 7-6

Deployment Scenarios

Connected Edge Storage is typically used when the camera is off network, or to save network bandwidth. Refer to the following use cases for more information:
- Network Bandwidth Savings, page 7-3
- Off-Network Cameras, page 7-4

Network Bandwidth Savings

If cameras are installed at a location where video is only required on demand, Connected Edge Storage can be used to dramatically reduce the required bandwidth and server storage. Video is saved on the camera storage device, such as an SD card, and delivered to the Media Server and end user only on demand. This eliminates the need for a locally-installed Media Server (Figure 7-1).

Instead of streaming video continuously, like most cameras, video is only sent when an event and/or request occurs.
This deployment scenario is useful when it is not critical to continuously monitor or record video.

**Off-Network Cameras**

Cameras that support on-device video storage can save recordings on the camera, and copy them to the Cisco VSM system at a later time. This feature is typically used when the camera is out of network range while recording.

For example, in Figure 7-2 a bus equipped with an IP (network) camera can save video recordings to the camera even when the bus is transporting passengers. When the bus returns to the depot, and is again in network range, the recordings can be copied to the Media Server that supports the camera. The copy action can be performed automatically when the bus camera rejoins the network, or an operator can manually trigger the copy action using the Operations Manager interface.
Figure 7-2  "Connected Edge Storage": Camera Recording on Device and Copy to a Media Server
Copy Options

Video that is saved to the camera’s SD card must be copied to the Cisco Media Server so it can be viewed and analyzed using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

The video can be copied manually based on a start and end time, or automatically copied when an event occurs. Video can also be merged based on the camera template recording schedule.

Table 7-2 summarizes the options to copy camera recordings:

<table>
<thead>
<tr>
<th>Copy Method</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>A Cisco VSM operator can manually copy video for a specific time-range. Any available video within that range is copied from the camera to the Media Server.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Manually Copy Camera Recordings</td>
</tr>
<tr>
<td>“Copy Camera Recordings”</td>
<td>Automatically copies a continuous recording to the Media Server based on the camera template’s recording schedule. After configuration, no user interaction is required. The recordings are copied to the Media Server when camera network communication is established (or re-established).</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Auto-Merge Recordings (Automatically Copy All Recording)</td>
</tr>
<tr>
<td>Automatic when an event occurs</td>
<td>Automatically copies the video for an event when the event occurs. When the action for an event is “Record for some time”, video for each event is automatically saved to the camera storage (such as an SD card) and to the Media Server.</td>
<td>Cisco Video Surveillance Operations Manager User Guide &gt; Using Advanced Events to Trigger Actions</td>
</tr>
</tbody>
</table>

Important Performance Considerations with Connected Edge Storage

Number of Supported Cameras

Due to bandwidth considerations, the number of cameras that can be supported by a Media Server will drop in half when all of the cameras on that server are configured with the “Auto-Merge recordings” option. We recommended a maximum of 10 cameras on a single Media Server be configured with “Auto-Merge recordings”. See the Cisco Video Surveillance Operations Manager User Guide for more information and configuration instructions.

- Cisco VSM Release 7.5 and highervcan support up to 100 cameras configured with “Auto-Merge recordings” on a single Media Server depending on the model of server and video data rate.
- See the “Auto-Merge Calculator” tool for guidance on using “Auto-Merge recordings” with more than 10 cameras on a single Media Server (to download the tool, go to the Cisco Video Surveillance Manager download page, select “Video Surveillance Manager Stand-alone Tools”, and download the “Auto-Merge Calculator” tool).
For cameras with camera storage configured with Manual Copy, there is no limit to the number of cameras on a single Media Server imposed by camera storage. The normal limits of 250 cameras and limits on recording bandwidth depending on video configurations of the cameras and server type still apply.

For example, when a camera configured with “Auto-Merge recordings” reconnects to the Media Server after a network outage, live video recording will resume and the camera will begin copying locally-stored video to the Media Server (to fill the recording gaps on the Media Server). Video is also copied from the camera at a rate that is at least 25% faster than real-time so that all of the video from an outage is copied from the camera before it is overwritten. This means that after an outage, the total bandwidth from the camera to the Media Server is more than 2X the video data rate until all of the video from the outage has been copied from the camera. Since the Media Server has a limit on total recording bandwidth, the use of “Auto-Merge recordings” will reduce the total number of cameras that can be supported on a Media Server. If all of the cameras on the Media Server are configured with “Auto-Merge recordings”, the number of supported cameras will drop by more than half.

Example Video and SD Card Configurations
The following tables show examples of video configurations and SD card sizes for 1RU and 2RU servers, and the maximum outage that can be supported by the “Auto-Merge Recordings” feature. If the outage exceeds the maximum, recorded video in the camera from the outage period will be lost.

Table 7-3  Video Configurations and SD Card Sizes: 1RU Servers

<table>
<thead>
<tr>
<th>Video and SD Card Configuration</th>
<th>Standard Cameras</th>
<th>Auto-Merge Cameras</th>
<th>Max Outage Duration (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Mbps 30 FPS 32GB SD Card</td>
<td>0</td>
<td>4</td>
<td>11.00</td>
</tr>
<tr>
<td>6 Mbps 30 FPS 16GB SD Card</td>
<td>0</td>
<td>4</td>
<td>5.00</td>
</tr>
<tr>
<td>6 Mbps 30 FPS 8GB SD Card</td>
<td>0</td>
<td>4</td>
<td>2.00</td>
</tr>
<tr>
<td>4Mbps 30 FPS 32GB SD Card</td>
<td>0</td>
<td>6</td>
<td>16.50</td>
</tr>
<tr>
<td>4Mbps 30 FPS 16GB SD Card</td>
<td>0</td>
<td>6</td>
<td>8.00</td>
</tr>
<tr>
<td>4Mbps 30 FPS 8GB SD Card</td>
<td>0</td>
<td>6</td>
<td>3.50</td>
</tr>
<tr>
<td>2Mbps 30 FPS 32GB SD Card</td>
<td>5</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>2Mbps 30 FPS 16GB SD Card</td>
<td>5</td>
<td>10</td>
<td>16.00</td>
</tr>
<tr>
<td>2Mbps 30 FPS 8GB SD Card</td>
<td>5</td>
<td>10</td>
<td>7.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 32GB SD Card</td>
<td>20</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 16GB SD Card</td>
<td>20</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 8GB SD Card</td>
<td>20</td>
<td>10</td>
<td>15.00</td>
</tr>
</tbody>
</table>
On-Camera Recording (Connected Edge Storage)

Chapter 7  Video Recording Options

Table 4  Video Configurations and SD Card Sizes: 2RU Servers

<table>
<thead>
<tr>
<th>Video and SD Card Configuration</th>
<th>Standard Cameras</th>
<th>Auto-merge Cameras</th>
<th>Max Outage Duration (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Mbps 30 FPS 32GB SD Card</td>
<td>10</td>
<td>10</td>
<td>11.00</td>
</tr>
<tr>
<td>6 Mbps 30 FPS 16GB SD Card</td>
<td>10</td>
<td>10</td>
<td>5.00</td>
</tr>
<tr>
<td>6 Mbps 30 FPS 8GB SD Card</td>
<td>10</td>
<td>10</td>
<td>2.00</td>
</tr>
<tr>
<td>4Mbps 30 FPS 32GB SD Card</td>
<td>25</td>
<td>10</td>
<td>16.50</td>
</tr>
<tr>
<td>4Mbps 30 FPS 16GB SD Card</td>
<td>25</td>
<td>10</td>
<td>8.00</td>
</tr>
<tr>
<td>4Mbps 30 FPS 8GB SD Card</td>
<td>25</td>
<td>10</td>
<td>3.50</td>
</tr>
<tr>
<td>2Mbps 30 FPS 32GB SD Card</td>
<td>75</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>2Mbps 30 FPS 16GB SD Card</td>
<td>75</td>
<td>10</td>
<td>16.00</td>
</tr>
<tr>
<td>2Mbps 30 FPS 8GB SD Card</td>
<td>75</td>
<td>10</td>
<td>7.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 32GB SD Card</td>
<td>175</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 16GB SD Card</td>
<td>175</td>
<td>10</td>
<td>23.50</td>
</tr>
<tr>
<td>1Mbps 15FPS 8GB SD Card</td>
<td>175</td>
<td>10</td>
<td>15.00</td>
</tr>
</tbody>
</table>

Additional Limitations

- MJPEG streams are not supported with the Connected Edge Storage feature.
- The maximum supported video bit rate for camera storage is 6Mbps.
- For Auto-Merge recordings, only video recorded in the last 24 hours can be auto-merged.
- When camera storage is used, the camera reserves 1GB of space on the SD card for buffering and it is not available for video recording. For example, only 15 GB is available on a 16GB SD card.
PART 4

Network Considerations
Cisco Video Surveillance Manager (Cisco VSM) deployments typically include servers, cameras, encoders, and users located in different networks. Network configuration for each of these devices must be correct or system errors will occur.

Review the Deployment Scenarios, page 4-1 for an overview of typical system configurations, then review the following topics to understand the network requirements, rules, and best practices for the servers, cameras, and other network devices in your deployment.

- Summary of Network NAT Support, page 8-2
- Server Network Considerations, page 8-3
  - Network Port Requirements, page 8-3
  - Default Ethernet Interface Settings, page 8-3
  - Rules for Server Reachability, page 8-4
  - Supported Ethernet Port Configuration Combinations, page 8-5
  - Using Dynamic Host Configuration Protocol (DHCP), page 8-6
  - DNS Server Support, page 8-7
  - Network Settings in a Virtual Machine (OVA File) Installation, page 8-7
- Understanding Device Conflicts, page 8-7
  - Devices with Duplicate IP Addresses, page 8-7
  - Conflicts During Camera Discovery, page 8-8
  - Allowing Duplicate Camera IP Addresses, page 8-8
- Resolving ID Mismatch Errors When Changing Camera IP Addresses, page 8-9
- Adding Cameras From Different Networks (NATs), page 8-11
  - Understanding Camera IP Addresses, page 8-11
  - Understanding Camera IP Address Conflicts, page 8-13
  - Camera Discovery and IP Addresses Conflicts, page 8-14
  - Manually Adding Cameras, page 8-15
- Camera Network Deployment Scenarios, page 8-15
  - Scenario 1: All Devices Are In the Same Network (NAT), page 8-15
  - Scenario 2: Cameras in Different NATs Use Static Access IP Addresses, page 8-17
  - Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 8-18
Summary of Network NAT Support

A typical Cisco VSM deployment includes servers, cameras, encoders, and users located in different networks, which requires video traffic and other data to be sent across network NAT boundaries. Although this is supported in Release 7.6 and higher, some configurations, such as Operations Manager HA server pairs, require devices to be in the same network NAT.

**Table 8-1 NAT Boundary Support**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Different NATs allowed?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Manager and Media Servers</td>
<td>Yes</td>
<td>Servers can be located in different NATs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Related Information</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Server Network Considerations, page 8-3</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Deployment Scenarios, page 4-1</a></td>
</tr>
<tr>
<td>Cameras and Media Servers</td>
<td>Yes</td>
<td>Cameras can be located in different networks from their associated Media Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Related Information</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Adding Cameras From Different Networks (NATs), page 8-11</a></td>
</tr>
<tr>
<td>Media Server HA pairs</td>
<td>No</td>
<td>The Primary Media Server should be located in the same NAT as its associated Redundant and Failover server.</td>
</tr>
<tr>
<td>Operations Manager HA server pair</td>
<td>No</td>
<td>Both Operations Manager servers in an HA configuration must be installed in the same network subnet. This ensures connectivity and data synchronization between the servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The two Operations Manager HA servers must use the same hostnames or IP addresses to reach all of the VSM servers they manage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Related Information</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Operations Manager (VSOM) HA, page 12-1</a></td>
</tr>
<tr>
<td>Encoders and Media Servers</td>
<td>No</td>
<td>Camera encoders should be installed in the same network as their associated Media Server.</td>
</tr>
</tbody>
</table>
Server Network Considerations

- Network Port Requirements, page 8-3
- Default Ethernet Interface Settings, page 8-3
- Rules for Server Reachability, page 8-4
- Supported Ethernet Port Configuration Combinations, page 8-5
- Using Dynamic Host Configuration Protocol (DHCP), page 8-6
- DNS Server Support, page 8-7
- Network Settings in a Virtual Machine (OVA File) Installation, page 8-7

Network Port Requirements

The following ports must be open in your network firewall to enable video and audio data communication between cameras, Cisco Media Servers and the Operations Manager servers (Table 8-2).

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Required Ports</th>
</tr>
</thead>
</table>
| TCP      | - HTTP (80), HTTPS (443), and SSH (22)  
- Ports 161, 2755, 61613, 61614, 61615, 61616, and 9090  
- RTSP (554) |
| UDP      | - 161, 16000:19999, and 5353  
- BOOTPC (68)  
- NTP (123) |

For example, Cisco Media Server streams all audio and video data to monitoring clients (PC workstations) from RTSP port 554. Cameras stream data to Media Servers using UDP port 16000:19999.

Default Ethernet Interface Settings

The default Ethernet port configuration for each Cisco VSM server is:
- Nic Port 0— configured with a private static IP address (http://192.168.0.200/)
- Nic Port 1— configured for DHCP (the IP address and other settings are received from a DHCP server, if available).

These settings are applied in new servers, or servers that have been restored using the USB recovery drive. Use either of these addresses to access the Cisco VSM Management Console and complete the Setup Wizard (see the “Using the Initial Setup Wizard” section on page 2-1). At least one of these interfaces must reachable from the network where the workstation is installed.
Rules for Server Reachability

- Dual-homed/NAT Configurations, page 8-4
- Server Reachability, page 8-4

Dual-homed/NAT Configurations

- Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service (including co-located servers). The Operations Manager server hostname can resolve to only one (correct) address. All users must be able to access that IP address.
- Dual-homed/NAT server configuration is supported only for stand-alone Maps, Metadata, and Media Servers.

Server Reachability

Stand-alone Maps, Metadata, or Media Servers must be added to Operations Manager using an IP address or hostname that can be accessed by all users.

For example, add the server using a hostname to ensure user requests resolve to the correct IP address if there is a NAT between users and the server.

\[\text{Note}\]

The hostname is usually resolved via DNS, but can also be resolved by configuring the user’s computer to resolve each server hostname.

- If a stand-alone Maps, Metadata, or Media Server is added to Operations Manager using an \textit{IP address}, then every user must be able to access that specific IP address (for example, they must be in the same NAT).
- If a stand-alone Maps, Metadata, or Media Server is added to Operations Manager using a \textit{hostname}, then every user must be able to resolve the hostname to an IP address that can be reached by the user.
Supported Ethernet Port Configuration Combinations

Cisco VSM servers support two Ethernet ports that can use a static IP address, receive network settings from a DHCP server, or be disabled. The supported port configuration depends on the services enabled on the server (Table 8-3).

Table 8-3  Supported Ethernet Port Configurations

<table>
<thead>
<tr>
<th>Server Services</th>
<th>Ethernet Port Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-located system (Operations Manager and additional services hosted on the same server)</td>
<td>Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.</td>
</tr>
<tr>
<td>Operations Manager-only system</td>
<td>Only one interface can be enabled (static or DHCP). The other interface must be disabled. Verify that the Operations Manager server hostname resolves to only one (correct) address. Dual-homed/NAT server configurations are not supported on any server running the Operations Manager service.</td>
</tr>
<tr>
<td>Stand-alone Maps, Metadata, or Media Servers</td>
<td>At least one Ethernet port must be enabled. The following combinations are supported:</td>
</tr>
<tr>
<td></td>
<td>• Both interfaces configured static.</td>
</tr>
<tr>
<td></td>
<td>• One interface static and the other disabled.</td>
</tr>
<tr>
<td></td>
<td>• One interface configured static and the other DHCP.</td>
</tr>
<tr>
<td>Notes:</td>
<td>A hostname must be configured on all servers. The hostname does not have to be accessible through DNS, but all servers must have a hostname configured (a hostname is required for some services such as ActiveMQ).</td>
</tr>
</tbody>
</table>

Usage Notes

- At least one static interface must be configured.
- A servers network settings can be modified using either the Cisco VSM Management Console or browser-based Operations Manager tool.
- Changing network settings can cause the server to restart system services. 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.
Using Dynamic Host Configuration Protocol (DHCP)

A DHCP server can be used to automatically assign network settings for a server, camera, or encoder.

Server DHCP

A DHCP server can be used to automatically assign the IP address, default gateway and the DNS server for a server Ethernet port. If DHCP is enabled, then the other network fields are disabled and the required settings must be provided by the DHCP server.

To manually assign the IP address, default gateway, or DNS server, de-select DHCP by selecting the Static IP option.

Note

If the Media Server interface used in the Operations Manager configuration is set to DHCP, the connection can be lost when the Media Server reboots and receives a different IP address. To restore communication, update the Operations Manager configuration in with the new Media Server IP address. To avoid this situation, we recommend using a DNS hostname for the DHCP interface, or using a static IP address.

Camera DHCP

DHCP also offers a convenient way to assign IP addresses to many cameras at once.

When using DHCP, it is important to configure the DHCP server properly. DHCP servers support assigning addresses to devices in these ways:

- Dynamic assignment—An IP address is assigned temporarily for the duration of a lease time. At the end of this time, the address expires and a new address is assigned.
- Automatic assignment—A camera is assigned a permanent IP address that is based on its MAC address.
- Static assignment—A system administrator must assign IP addresses based on MAC addresses of devices and enter the IP addresses into the DHCP server.

With dynamic assignment, an IP address can change when the lease expires. In general, this event causes a short loss in video while the IP address changes and streaming resumes. However, in some cases, such as if the IP address changes during certain administrative operations or during a failover, VSM is not informed of the address change and loses connectivity with the camera until the camera is reset. To avoid this situation, Cisco recommends that the DHCP server be configured with automatic assignment. If dynamic assignment must be used, Cisco recommends that a long lease time be configured.

Note

DHCP is required for using Medianet camera discovery in Cisco VSM 7.x. See Discovering Cameras on the Network, page 14-3 for more information.
DNS Server Support

We recommend configuring all VSM servers in DNS. Up to three DNS servers can be configured (the Linux OS supports up to three DNS servers).

Co-located VSOM/Media Servers must be in DNS to allow users to stream video from that server.

Network Settings in a Virtual Machine (OVA File) Installation

The default network settings, including the server address, can be changed during the installation of a virtual machine (VM) on the Cisco Unified Computing System (UCS) platform. This is done if you cannot access either of the default addresses with a web browser.

If necessary, see your system administrator for the address assigned to the server using the guest OS console.

See the “Configuring the Network Settings” section of the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for more information.

Understanding Device Conflicts

If a server, camera or encoder is added to Cisco VSM with duplicate settings, such as a duplicate IP address, an error can occur. Review the following information to understand how to avoid, resolve, or allow such conflicts:

- Devices with Duplicate IP Addresses, page 8-7
- Conflicts During Camera Discovery, page 8-8
- Allowing Duplicate Camera IP Addresses, page 8-8

Devices with Duplicate IP Addresses

By default, servers, encoders, or cameras with duplicate IP addresses are not allowed.

If an server or device is added with a duplicate IP address (the address is the same as an existing device), the new entry will display an ID collision issue. For example:

- Devices manually added with a duplicate IP address will be placed in the Enabled: Critical state.
- Discovered cameras will be placed in the Pending Approval list.

To resolve the issue, do one of the following:

- Use the Operations Manager to configure the server or device with an unused IP address.
- Directly connect to the device or server interface and enter a unique IP address, or ensure that the device can receive a reachable address from a DHCP server. The camera IP address must be reachable by the Media Server to which it is assigned.
- Use the Replace Camera or Replace Server option to transfer the old settings to the new device (see the Cisco Video Surveillance Operations Manager User Guide).
- Delete the camera, encoder, or server and re-add it with a unique IP address.
Understanding Device Conflicts

- Enable the **Allow Duplicate IP Address** system setting to allow servers and devices to be added with duplicate IP addresses. For example, Media Servers that are installed in NATs that use the same Access IP (NAT) address. See the *Cisco Video Surveillance Operations Manager User Guide* for more information.

Conflicts During Camera Discovery

Cameras are identified in Cisco VSM discovery by the device IP Address, and serial number, mac address/hardware ID. If a camera is discovered with values in these fields that already exist in the Cisco VSM configuration, the camera records will either be merged, or placed in a collision state.

- If some identity fields in a discovered camera and existing camera are a perfect match, but some fields are empty, then the records are merged. For example, if a camera in Cisco VSM includes only a name and MAC address, and a discovered camera has the same MAC address plus additional fields for serial number and IP address, then the two records are merged into a single camera entry.
- If both the Cisco VSM camera and a discovered camera include identity fields that do not match, both cameras are placed in a collision state. You must replace or delete one of the cameras to remove the conflict.

Open the camera **Status** tab on the configuration page to view more information.

- The device overall status is **Enabled: Critical**.
- Click the link next to the **Hardware** category to open a pop-up that details the collision.
- An **Alert** is generated for “identity collision”.

- If the discovered camera uses DHCP settings, and only the IP address is in conflict, then the IP address of the discovered camera is used. If the discovered camera uses a static IP address, however, then the camera entries are in conflict.

Open the camera **Status** tab on the configuration page to view more information.

**Note**

Settings such as name, template, location, media-server associations are configurations in the Operations Manager and are not merged or overwritten by discovered settings.

See also the “Adding Cameras From Different Networks (NATs)” section on page 8-11.

Allowing Duplicate Camera IP Addresses

By default, servers, encoders, or cameras with duplicate IP addresses are not allowed and will result in an error. See *Devices with Duplicate IP Addresses, page 8-7* for more information.

If your network configuration requires that devices be added with duplicate IP addresses, you can enable the **Allow Duplicate IP Address** system setting. This setting allows multiple cameras with the same access IP address to be added to the Operations Manager configuration. For example, cameras with the same IP address can be added to different Media Servers in different locations.

See the following for more information:

- **Adding Cameras From Different Networks (NATs), page 8-11**
- **Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 8-18**
Resolving ID Mismatch Errors When Changing Camera IP Addresses

If cameras are configured with IP addresses (and not hostnames), and those IP addresses change, a hardware id mismatch issue can occur and the camera will be placed in the Enabled: Critical state (red). This occurs because the camera’s hardware ID no longer matches the device IP address. To clear this issue, correct the network configuration for each affected camera. For example:

- Scenario 1: Cameras Configured with DHCP IP Addresses, page 8-9
- Scenario 2: Cameras Configured with a Static IP Addresses, page 8-10

Note

- Medianet cameras must be configured for DHCP. Cameras that do not support Medianet can only be added using a static IP address. See Using Dynamic Host Configuration Protocol (DHCP), page 8-6 for more information.
- The following scenarios can also occur for cameras configured with hostnames, if the DNS entry does not update with the correct hostname to IP address mapping.

Scenario 1: Cameras Configured with DHCP IP Addresses

Cameras that revive a new DHCP-provided IP address after reboot will be placed in Enabled: Critical state with a hardware ID mismatch issue. This is because the IP address no longer matches the hardware address configured in the Operations Manager. This occurs for each camera where the IP address was changed.

To resolve this issue:

Cisco Cameras

The new IP address is automatically updated in Operations Manager for Cisco cameras configured with DHCP. To clear the error message, choose Repair Configuration from the Device Settings menu.

Step 1
Open the camera configuration page.

Step 2
Select the Status tab and verify the following:
- The device overall status is Enabled: Critical.
- Click the link next to the Hardware category to open a pop-up window.
- Verify that a Hardware ID Mismatch issue occurred.

Step 3
Select Device Settings > Repair Configuration to clear the issue.

Step 4
Verify that the camera status changes to Enabled: OK (green).

Non-Cisco Cameras

You must manually enter the correct IP address in the camera configuration for non-Cisco cameras configured with DHCP.

Step 1
Open the camera configuration page in Operations Manager.
Resolving ID Mismatch Errors When Changing Camera IP Addresses

Step 2  Select the **Status** tab and verify the following:

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up window.
- Verify that a *Hardware ID Mismatch* issue occurred.

Step 3  Select the **General** tab.

Step 4  Under Access Information, enter the correct IP address for the device.

- This is the setting used by Operations Manager to communicate with the device,
- The IP address stored in Operations Manager must be the same as the device configuration.

Step 5  Verify that the camera status changes to *Enabled: OK* (green).

Scenario 2: Cameras Configured with a Static IP Addresses

If cameras are configured with a static IP address, and that address is changed in the camera’s device user interface, the device is placed in *Enabled: Critical* state with a hardware ID mismatch issue. This is because the IP address no longer matches the hardware address configured in the Operations Manager. This occurs for each camera where the IP address was changed.

- If another camera has the same IP address, an *ID collision* issue occurs. See Understanding Device Conflicts, page 8-7 for more information and to resolve the issue.
- If the camera’s IP address is unique, but no longer matches the entry in the Operations Manager, you must correct the entry on the camera configuration page.

Procedure

Step 1  Open the camera configuration page in Operations Manager.

Step 2  Select the **Status** tab and verify the following:

- The device overall status is *Enabled: Critical*.
- Click the link next to the *Hardware* category to open a pop-up window.
- Verify that a *Hardware ID Mismatch* issue occurred.

Step 3  Select the **General** tab.

Step 4  Under Access Information, enter the correct IP address for the device.

- This is the setting used by Operations Manager to communicate with the device,
- The IP address stored in Operations Manager must be the same as the device configuration.

Step 5  Verify that the camera status changes to *Enabled: OK* (green).
Adding Cameras From Different Networks (NATs)

This document describes how to add cameras that are installed in different network (NAT) than the Cisco VSM Operations Manager.

Contents
- Overview, page 8-11
  - Understanding Camera IP Addresses, page 8-11
  - Understanding Camera IP Address Conflicts, page 8-13
  - Camera Discovery and IP Addresses Conflicts, page 8-14
  - Manually Adding Cameras, page 8-15
- Camera Network Deployment Scenarios, page 8-15
  - Scenario 1: All Devices Are In the Same Network (NAT), page 8-15
  - Scenario 2: Cameras in Different NATs Use Static Access IP Addresses, page 8-17
  - Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 8-18

Overview

Review the following topics to understand the two different IP addresses assigned to cameras, and how the Cisco VSM Operations Manager determines if a duplicate entry exists when adding the new device.

- Understanding Camera IP Addresses, page 8-11
- Understanding Camera IP Address Conflicts, page 8-13
- Camera Discovery and IP Addresses Conflicts, page 8-14
- Manually Adding Cameras, page 8-15

Understanding Camera IP Addresses

Each surveillance camera has two IP addresses:

- A Private (NIC) IP address—used for communication within the private network (NAT boundaries).
- An Access (NAT) IP address—used for communication between the camera and external networks.

Note
If all cameras and servers are in the same network, then the Private (NIC) IP address and Access (NAT) IP address are the same. See Scenario 1: All Devices Are In the Same Network (NAT), page 8-15.
The network router uses network address translation (NAT) to route data from the private NIC address of a device (camera) to and from external networks. For example, in Figure 8-1, a request from the Cisco VSM Operations Manager is sent to the camera’s access (NAT) IP address. The network router forwards that data to the camera’s private (NIC) IP address.

To ensure data is sent to the correct device, the Operations Manager normally requires that each camera’s access (NAT) IP address be unique (by default). If a camera is added or discovered, and a device entry with the same access (NAT) IP address already exists, the camera may be merged with an existing record, or an error can occur. See the “Understanding Camera IP Address Conflicts” section on page 8-13.

This document describes the following scenarios to avoid camera IP address conflicts:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>All devices are in the same network. Cameras are assigned static IP addresses or managed by a DHCP server that avoids IP address conflicts.</td>
<td>Scenario 1: All Devices Are In the Same Network (NAT), page 8-15</td>
</tr>
</tbody>
</table>
Understanding Camera IP Address Conflicts

A camera IP address conflict occurs if the device is assigned an IP address that is already configured on another camera that was (previously) added to Cisco VSM.

If a camera is added or discovered with a duplicate access (NAT) IP address, the following rules apply:

**Cameras added with a DHCP-provided IP address**

If the discovered camera uses DHCP settings, and only the IP address is in conflict, then the IP address of the discovered camera is used. The device status will be *Critical* with a “Hardware ID mismatch” issue. To resolve this issue, select *Repair Configuration* from the *Device Settings* menu.

For example, if a Cisco camera is rebooted and receives a new DHCP IP address that is already used by another camera in Cisco VSM, the camera will use that IP address, but the device status will be *Critical* with a “Hardware ID mismatch” issue. Select *Repair Configuration* from the *Device Settings* menu to change the device status to *Enabled:OK* (green).

**Cameras added with a static IP address**

If the discovered camera uses a static IP address, however, then the camera entries are in conflict.

- If the *Allow Duplicate IP addresses* system setting is enabled, the conflict is ignored and the camera is added to Cisco VSM.
- If the *Allow Duplicate IP addresses* system setting not enabled (default), then both cameras are placed in a collision state. You must replace or delete one of the cameras to remove the conflict, or use the Operations Manager to reconfigure one of the cameras with a unique IP address.

For example, if you configure a static IP address on a camera using the device UI, and then add that camera to Cisco VSM, the camera is be in the *Critical* state with a “Hardware ID mismatch” issue if the IP address is already used by another Cisco VSM camera.

To resolve this issue, use the Operations Manager to reconfigure the camera with a unique IP address. The device status should change to *Enabled:OK* (green).

**Viewing Camera Status**

To view more information about the IP address conflict, use the camera Status page to view the “identity collision” alert.

**Table 8-4 Camera IP Addresses: Network (NAT) Deployment Scenarios (continued)**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameras in different networks are assigned unique static access (NAT) IP addresses.</td>
<td>Scenario 2: Cameras in Different NATs Use Static Access IP Addresses, page 8-17</td>
</tr>
<tr>
<td>Cameras in different networks are assigned duplicate access (NAT) IP addresses.</td>
<td>Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 8-18</td>
</tr>
</tbody>
</table>

**Scenario More Information**

Cameras in different networks are assigned unique static access (NAT) IP addresses.

Cameras in different networks are assigned duplicate access (NAT) IP addresses.

The system setting *Allow duplicate IP addresses* is enabled to allow cameras with duplicate IPs to be added.

The Operations Manager ignores IP address conflicts and allows the cameras to be added to the configuration.

**Step 1**
Select *Cameras*.

**Step 2**
Select a location and select the camera in conflict.
Step 3 Select the Status tab.

- The device overall status is *Enabled: Critical*.
- Click the link next to the Hardware category to open a pop-up that details the collision.
- An Alert is generated for “identity collision”.

See the “Understanding Camera Conflicts During Discovery” section on page 15-3 for more information.

Camera Discovery and IP Addresses Conflicts

**Note**

Camera discovery occurs when an IP camera is discovered on the network and added to the Cisco VSM configuration. Camera discovery can occur automatically when the camera is added to the network, or manually triggered by an administrator. During camera discovery, Cisco VSM checks to see if a duplicate camera configuration exists. Cameras are identified by the device IP Address, and serial number/MAC address/hardware ID. If a camera is discovered with values in these fields that already exist in the Cisco VSM configuration, the camera records will either be merged, or placed in a collision state. See the “Discovering Cameras on the Network” section on page 15-1 for more information.

Camera discovery manages camera IP addresses using the following process:

1. The Media Server detects that a camera is behind a private network and uses an access (NAT) IP address.
2. The Operations Manager determines if another camera already in the system uses the same access (NAT) IP address.
   a. If a duplicate access (NAT) IP address is found on a DHCP-enabled camera, then the discovered camera is merged with the existing camera entry. The camera's private (NIC) IP address is included in the merged entry. Select Device Settings > Repair Configuration to change the device status to *Enabled:OK* (green).
   b. If the camera uses a static IP address that is not used by another Cisco VSM camera, the camera is added normally (a collision does not occur).
   c. If the camera uses a static IP address that is already used by another Cisco VSM camera, a collision will occur.
      - If the Allow Duplicate IP Address system setting is not enabled (default), both cameras are placed in a collision state and you must replace or delete one of the cameras to remove the conflict. See the “Understanding Camera IP Address Conflicts” section on page 8-13.
      - If the Allow Duplicate IP Address system setting is enabled, the new camera with the duplicate access (NAT) IP address is added to Cisco VSM.

When a camera is successfully added to Cisco VSM, both the access (NAT) IP and private (NIC) IP are added to the camera entry in the Operations Manager.

**Tip**

If auto-provisioning is enabled for the discovered camera model, the camera is also updated with settings for template, user credential, etc. See the Cisco Video Surveillance Operations Manager User Guide for more information.
Manually Adding Cameras

Cameras are manually added to Cisco VSM using the access (NAT) IP address.

If duplicate access (NAT) IP address is used, a collision will occur.

- **If the Allow Duplicate IP Address system setting is not enabled (default), both cameras are placed in a collision state and you must replace or delete one of the cameras to remove the conflict. See the “Understanding Camera IP Address Conflicts” section on page 8-13.**
- **If the Allow Duplicate IP Address system setting is enabled, the new camera with the duplicate access (NAT) IP address is added to Cisco VSM.**

Both the access (NAT) IP and private (NIC) IP are added to the camera entry in the Operations Manager.

Camera Network Deployment Scenarios

- **Scenario 1: All Devices Are In the Same Network (NAT), page 8-15**
- **Scenario 2: Cameras in Different NATs Use Static Access IP Addresses, page 8-17**
- **Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses, page 8-18**

**Scenario 1: All Devices Are In the Same Network (NAT)**

In the most basic scenario, all cameras and servers are in the same network (NAT). This includes the video surveillance cameras, Operations Manager, and Media Servers (Figure 8-2).

In this single-network scenario, the private (NIC) and access (NAT) IP addresses are the same for each camera.

---

**Note**

Only the access (NAT) IP address is entered and displayed in the camera’s configuration page.
Each camera should have a unique IP address, or a collision ID can occur. See the “Understanding Camera IP Address Conflicts” section on page 8-13 for more information.

Figure 8-2 **Scenario 1: All Devices in the same Network (NAT)**
Scenario 2: Cameras in Different NATs Use Static Access IP Addresses

In this scenario, multiple groups of cameras are installed in different networks. The cameras in each network are assigned the same set of private (NIC) IP address. Each camera, however, is also assigned a unique static access (NAT) IP address (Figure 8-3).

In this scenario:

- The camera is added using the Access (NAT) IP addresses. The Access (NAT) appears in the camera page of the Operations Manager UI.
- Only Access (NAT) IP is checked for duplicate. The Private (NIC) address is ignored during the duplicate check.
- The Access (NAT) IP addresses is static and unique, so a collision ID will not occur.
- The Private (NIC) address is taken from the IP header and added to the config.

Note

- This scenario is supported when manually adding a camera, or for automatic discovery of Medianet-enabled cameras.
- User-initiated discovery of cameras (non-Medianet devices) is not supported since the Operations Manager cannot determine that the cameras are behind a NAT (since DHCP is not used).
Scenario 3: Cameras in Different NATs Have Duplicate Access IP Addresses

In this scenario, multiple groups of cameras are installed in different networks. The cameras in each network are assigned the same set of private (NIC) IP address. The access (NAT) IP address for each camera, however, may be a duplicate of another camera. By default, can cause a collision ID error. To avoid this, (Figure 8-4).

Figure 8-4 Scenario 3: Cameras in Different Networks with Duplicate “Access” (NAT) IP addresses

In this scenario:

- The Access (NAT) IP addresses is added or discovered.
- Only Access (NAT) IP is checked for duplicates. If a duplicate exists, a collision ID can occur. See the “Understanding Camera IP Address Conflicts” section on page 8-13.
- Select the **Allow Duplicate IP Addresses** system setting to allow duplicates. Duplicate camera entries will be ignored and the camera will be added.
- The Private (NIC) address is taken from the IP header and added to the camera config.
Understanding NTP Configuration

The server time synchronizes server operations, defines recording timestamps and backup schedules. To ensure correct playback and system operation, we strongly recommend using a network time protocol (NTP) for all servers and devices.

Note
Video is recorded at GMT, but displayed in local time (the time where the user is viewing the video). For example, if a user is viewing EST video from a PST time zone, the video will display the PST time.

Refer to the following topics for more information:

- Recommended (and Default) NTP Configuration, page 9-2
- NTP Usage Notes, page 9-3
- Configuring Media Servers with a User-Defined NTP Server, page 9-4
- Configuring Cameras with a User-Defined NTP Server, page 9-5
- Defining the NTP Setting During Camera Auto-Discovery, page 9-6
Recommended (and Default) NTP Configuration

In the default and recommended NTP configuration, the Operations Manager is configured with an NTP server, and all other servers, cameras and encoders use the Operations Manager as their NTP server. This ensures that all devices, recordings, timestamps, alerts, and other resources are synchronized.

In Figure 9-1, the cameras use their Media Servers as the NTP server, and the Media Servers use the Operations Manager as the NTP server. Since these are the default settings, no user configuration is required except to (optionally) enter a custom NTP server address for the Operations Manager server.

**Figure 9-1** Recommended (and Default) NTP Configuration

![Diagram of NTP configuration]

**Table 9-1** Recommended NTP Configuration

<table>
<thead>
<tr>
<th>Server/Device</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Manager server</td>
<td>Enter a “User-Configured” NTP server for the Operations Manager server, including servers that are co-located with other services, such as a Media Server and/or Maps server.</td>
</tr>
<tr>
<td>Stand-alone servers</td>
<td>Use “Automatic” mode for all other servers. The Operations Manager is used as the NTP server, ensuring that the date and time on all servers are in sync.</td>
</tr>
<tr>
<td>Cameras and encoders</td>
<td>By default, cameras and encoders use the Media Server to which they are assigned as the NTP server. This ensures that the recording timestamps and schedules are in sync.</td>
</tr>
</tbody>
</table>

**Note** The encoder NTP setting cannot be changed.
NTP Usage Notes

- Enter NTP Server names or IP addresses separated by space or comma.
- **Automatic** mode can only be used after NTP is configured on the Operations Manager server.
- The server will reboot if any changes are made to the NTP settings using the Operations Manager UI.
- Changes to the server time can affect video recording schedules and timestamps.
- A warning alert is generated if the time difference between the server and Operations Manager is more than 2 minutes.
- A warning message is also displayed to operators when logging in if the time difference between their workstation and the server is more than 2 minutes.
- You can modify the NTP information for up to 10,000 cameras at a time.
- The NTP servers configured on a device are displayed in the device configuration page (under NTP Information).
- NTP settings can be configured on camera only if the camera model supports NTP configuration.
- The number of NTP servers configured on a camera are limited to the number supported by the camera model. For example, if a camera model only supports a single NTP server setting, and you attempt to add three NTP servers, the configuration will be rejected.
- Never modify the time and NTP settings using the Linux CLI. Settings made using the Linux CLI can result in inconsistent system performance and other issues.
Configuring Media Servers with a User-Defined NTP Server

In some situations, you may need to use different NTP server settings than the default and recommended version. This may be necessary based on proximity of the Media Servers. For example: if your deployment spans numerous countries or timezones, the Media Servers may need to use local NTP servers.

In Figure 9-2, a Media Server in a distant location is assigned a “user defined” NTP server.

Refer to the Cisco Video Surveillance Operations Manager User Guide for configuration instructions.
Configuring Cameras with a User-Defined NTP Server

If your configuration requires that cameras use an NTP server that is not the Media Server, you can enter a custom NTP server address for a single camera, or for multiple cameras.

Figure 9-3 shows cameras that are configured with a custom NTP server.

Refer to the Cisco Video Surveillance Operations Manager User Guide for configuration instructions.
Defining the NTP Setting During Camera Auto-Discovery

By default, the Media Server is used as a camera’s NTP server when the device is added to Cisco VSM (see Figure 9-1).

When a camera is discovered on the network, the Media Server is also used as the camera’s NTP server by default. To override this option, and retain any NTP address(es) previously configured on the device, deselect the Use Media Server as NTP option in the auto configuration settings (Figure 9-4).

![Figure 9-4 Device Auto Configuration](image)

If an NTP server is not configured on the device, you must update the camera settings to either enter an NTP server address or select Use Media Server as NTP.

- This setting is displayed only for camera models that support NTP.
- You must belong to a user group with Cameras permission.
- See the “Configuring Cameras with a User-Defined NTP Server” section on page 9-5 for information to define a new NTP server for one or more cameras.

Note

Auto-configuration applies a set of basic configurations to cameras that are discovered on the network. Auto-configuration is disabled for all camera models by default. See Discovering Cameras on the Network, page 15-1 for more information.
PART 5

Server Features and Options
Server Storage

- Storage Types: SAN (FC & iSCSI), NAS Considerations, page 10-1
- Extending Video Archive Retention Using Long Term Storage Servers, page 10-2

Related Information
- Determining the Required Resources, page 6-1

Storage Types: SAN (FC & iSCSI), NAS Considerations

External storage systems can be used to provide video recording storage options and larger capacities than individual servers provide. Surveillance video recording is normally non-stop streaming and recording of video data so the storage system video is recorded to must be able to handle the continuous writing of video data 24x7x365. To accomplish the sustained streaming and writing of video data SAN storage systems connected through Fiber Channel is recommended for most uses. iSCSI connected storage systems can be as a virtual drive configured through virtual machine’s hypervisor.

NAS storage systems are not recommended due to lower performance handling continuous video recording, and can require additional management to ensure the shared storage is able to continue to provide the capacity allocated to the virtual machines.
Extending Video Archive Retention Using Long Term Storage Servers

A Long Term Storage (LTS) server allows you to automatically transfer recorded video from the Primary server to a LTS server. This frees the limited space on the Primary server, and provides a dedicated resource to store and play back old recordings.

- Recordings remain in the Primary and Redundant servers even if they are archived to an LTS server. The recordings are removed from the Primary and Redundant servers based on the Retain settings available in the camera or template configuration page (Retain continuous recordings and Retain event recordings).
- Recordings are removed from the LTS server according to the settings described in the Cisco Video Surveillance Operations Manager User Guide.
- Both stream A and stream B can be backed up.
- Backups are performed on an automatic schedule (for example, once a week at midnight).

Tip

You can also click Backup Now from the Primary or Redundant server to immediately back up the recordings to the LTS server. Select the Advanced tab and click Backup Now.
Using Dynamic Proxy to Monitor Video From Low-Bandwidth Sites

- Dynamic Proxy Overview, page 11-1
- Dynamic Proxy Design Considerations, page 11-3
- Dynamic Proxy Frames to Skip, page 11-3
- Configuring Dynamic Proxy, page 11-4

**Dynamic Proxy Overview**

When cameras and their associated Media Servers are located in Site with limited outgoing connectivity (such as an offshore oil platform), the Dynamic Proxy (DP) feature can be used to reduce the amount video data going out from that remote Site (Figure 11-1).

The Dynamic Proxy (DP) feature provides this service by retrieving video from the remote Media Servers and delivering it to the end users. The DP minimizes the amount of bandwidth used to deliver video data from the remote Site while allowing multiple users to access that video data.
Dynamic Proxy Overview

Figure 11-1 Dynamic Proxy Example

For example, in Figure 11-1, an offshore oil platform has a set of IP cameras and Media Servers. Any requests coming from users within that Site can be serviced by those on-Site Media Servers. Since the internal network is robust, the video is delivered at high resolution.

However, since this offshore oil platform has limited bandwidth to send data to on-shore monitoring Sites, requests from off-Site users would quickly consume the available outgoing bandwidth.

When the Dynamic Proxy feature is enabled, however, requests for video from off-Site (onshore) clients can be intercepted and serviced by the Dynamic Proxy. This Dynamic Proxy can collect a single video stream from the off-shore Site and deliver it to multiple users onshore.

For example:

- The Dynamic Proxy establishes secure communication with the source Media Server, retrieves the video, and displays it to the off-Site user(s) who requested it.
- The Dynamic Proxy service scales down the audio/video quality to accommodate small network pipe between the Media Server and the Dynamic Proxy server.
- The Dynamic Proxy service is only available for live video streams.
- The Dynamic Proxy servers do not support Failover. If a Dynamic Proxy server goes down or is unavailable, the user must re-request the video stream. The video will be served by a different Dynamic Proxy server, if configured.
- PTZ commands can be used by users inside and outside a Site since PTZ commands use a small amount of bandwidth and are sent directly to the Media Server.
Dynamic Proxy Design Considerations

When using Dynamic Proxy, observe the following:

- The maximum number of viewers per Dynamic Proxy stream is 20 viewers.
- The maximum latency between a Media Server and Dynamic Proxy Server is 4 seconds. This is long enough to allow the use of a satellite link between a central site and remote location.
- The Dynamic Proxy server supports only live video. Access to recorded video goes directly to the Media Server where the recorded video is stored. This doesn’t benefit from bandwidth savings through the proxy server.
- Camera Controls like PTZ are not supported through the Dynamic Proxy server. These commands go directly to the Media Server that is hosting the camera that is the intended target of the command.
- Proximity based DP Server selection is not supported. This means if a user logs in from the Milpitas Site and is accessing a camera in San Jose and if there are Dynamic Proxy servers in North Carolina and one in San Jose, the Operations Manager will randomly pick one of the DP Servers.
- A camera can only be proxied by a single Dynamic Proxy Server at a time.

Dynamic Proxy Frames to Skip

Observe the following guidelines to define the number of frames to skip when configuring a Dynamic Proxy server.

**Table 1 Frames To Skip (Site Settings)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MJPEG Max Framerate To Skip</td>
<td>(Optional) Stream thinning to be carried out for MJPEG streams. Must be set based on bandwidth availability.</td>
</tr>
<tr>
<td></td>
<td>All MJPEG frames are IFrames. Depending on the frame rate of the original stream, skip values are supported when the cumulative frame rate is greater than or equal to 0.1 fps. Therefore, the maximum value is 10 times the MJPEG stream's framerate.</td>
</tr>
<tr>
<td></td>
<td>The supported values are from 1 - 300.</td>
</tr>
<tr>
<td></td>
<td>For example, if the original frame rate of the MJPEG stream is ( o_{fr} ), then the “MJPEG Max Framerate To Skip” can be any value, ( x ), where ( o_{fr}/x \geq 0.1 \text{ fps} ).</td>
</tr>
<tr>
<td></td>
<td>For example, for 10fps, it is 100, for 30 fps, it is 300, for 0.1fps, it is 10, etc.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting is enabled only if the Dynamic Proxy service is enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Max IFrames To Skip</th>
<th>(Optional) The number of IFrames to skip for a video feed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The minimum and maximum skip rates vary depending on the video stream format:</td>
</tr>
<tr>
<td></td>
<td><strong>MPEG4/H.264 Streams</strong></td>
</tr>
<tr>
<td></td>
<td>The minimum and maximum values are 1– 9 (true only for cameras sending 1IFrame per second).</td>
</tr>
<tr>
<td></td>
<td>MPEG4 and H264, setting skip results in a stream with only IFrames. Most cameras send 1 IFrame per second. If the stream (regardless of frame rate) is sending 1 IFrame per second, the maximum skip is 9.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This setting is enabled only if the Dynamic Proxy service is enabled.</td>
</tr>
</tbody>
</table>
Configuring Dynamic Proxy

See the Cisco Video Surveillance Operations Manager User Guide for detailed instructions to configure dynamic proxy servers. This includes:

- Dynamic Proxy requirements
- Configuring Sites
- Detailed configuration instructions
Server High Availability

- Operations Manager (VSOM) HA, page 12-1
  - Understanding Operations Manager HA, page 12-2
  - Requirements, page 12-9
- Media Server Redundancy and Failover, page 12-6
  - Understanding Redundant and Failover Servers, page 12-6
  - Understanding Media Server Failover, page 12-8
  - Requirements, page 12-9
  - Determining HA Server Scalability, page 12-10
  - Failover Server Recommended Load and Limitations, page 12-10

**Operations Manager (VSOM) HA**

Two Operations Manager servers can be configured as a redundant pair for high availability (HA). Since the Operations Manager is responsible for configuring and coordinating the entire Cisco Video Surveillance deployment, this helps ensure uninterrupted system access for users and administrators.

To configure Operations Manager HA, install two servers: a Master server and a second Peer server. All configurations, data, and logs on the Master server are automatically replicated on the Peer server. If the Master server goes down or is unavailable, the Peer server is ready to take control with minimal impact.

Review the following topics before deploying Operations Manager HA.

- Understanding Operations Manager HA, page 12-2
- Requirements, page 12-9
Understanding Operations Manager HA

Operations Manager HA is achieved by installing two stand-alone Cisco VSM Operations Manager servers, and configuring one as the Master server, and the other as the Peer server (Figure 12-1). A virtual IP address is shared by both servers, and used by users (video monitors, administrators and other users) to access the Cisco Video Surveillance system. This configuration provides full operations and administrative function at all times.

Figure 12-1  Operations Manager HA: Server 1 is the Master Server

In Figure 12-1, users enter the virtual hostname/IP address to connect to the Cisco VSM Operations Manager. Server 1 acts as the Master server, receiving and managing all user and system requests. All data and configuration changes are automatically synchronized with the Peer server (server 2) to ensure it is ready to take over if a failover occurs.

The Peer polls the Master server regularly to verify connectivity. If the Peer does not receive a response, the Master is assumed to be down or offline and the Peer assumes the Master role (Figure 12-2). The Peer server immediately takes control of the system, and the virtual hostname/IP address is redirected to the new Master server.

Note  In the Figure 12-2 example, Server 1 assumes the Peer role when it comes back online, and retains that role until another failover occurs (admins can also force a failover if necessary).
Figure 12-2  After Operations Manager Failover: Server 2 is the Master Server

User Interfaces

The following user interfaces (UIs) access Cisco VSM video using the shared virtual IP address:

- Operations Manager (browser-based UI)—enter the virtual hostname/IP address in an Internet Explorer browser window.
- Cisco SASD (desktop application)—enter the virtual hostname/IP address at the login prompt.
- Custom applications—monitoring applications that use the Cisco VSM APIs access the Operations Manager using the virtual hostname/IP address.
# Requirements

Before you configure Operations Manager HA, verify that the following requirements are met.

**Note**  The VSOM High Availability configuration page appears only if the server is a stand-alone Operations Manager and is running a supported OS (such as RHEL 6.4).

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure Operations Manager HA, admins must belong to a User Group with permissions for Servers &amp; Encoders.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>See the “Adding Users, User Groups, and Permissions” section on page 4-1 for more information.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>Two standalone physical or virtual servers must be installed on the same network.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>– Supported physical servers: CPS-UCS-1RU-K9 or CPS-UCS-2RU-K9</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>– Supported virtual machines: VMs deployed using the Cisco VSM release 7.5 or 7.6 OVA templates.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>Note Any data on the server used as the Peer server will be deleted and replaced with the data from the Master server.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>We recommend two CPS-UCS-2RU-K9 servers for best performance.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• Performance issues can occur using the CPS-UCS-1RU-K9 servers for Operations Manager HA since performance issues (such as slowness) may occur.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• Do not mix a CPS-UCS-2RU-K9 server with a CPS-UCS-1RU-K9 server.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>Additional server requirements and recommendations:</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• Stand-alone servers—Only stand-alone physical or virtual servers are supported in an HA configuration. The Operations Manager servers can not be co-located with other server services, such as a Media Server.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• Operating system—Red Hat 6.4 64 bit OS only (SUSE and Red Hat 5.8 are NOT supported).</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• We recommend that both servers have the same hardware specifications such as processor, hard disk storage, and other attributes. For example, two CPS-UCS-2RU-K9 servers.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• We do not recommend using Cisco UCS E-series platform servers for Operations Manager HA.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• Both servers used for HA must be fully up and running prior to configuring HA or replacing the Peer server. Verify that there are no pending jobs (of any kind) in the Peer server.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>Split Brain recovery support:</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• At least one Media Server must be added to the Split Brain Configuration to support recovery if communication between the Master and Peer server is lost.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
<tr>
<td>• See Cisco Video Surveillance Operations Manager User Guide.</td>
<td><img src="%E2%9C%93" alt="✓" /></td>
</tr>
</tbody>
</table>
Network requirements:

- Subnet—Both servers must be in the same network subnet. This ensures connectivity and data synchronization between the servers.
- NIC port—Both servers must be connected to the network using the same NIC port: for example, Eth0. Only a single Ethernet port can be active (either Eth0 or Eth1).
- Three IP addresses/hostnames are required:
  - An IP address/hostname for the Master server Ethernet (NIC) port.
  - An IP address/hostname for the Peer server Ethernet (NIC) port.
  - A virtual IP address that is shared by both servers.

**Note** End-users should always use the virtual IP address to access the Operations Manager since it will still work even in a failover occurs. Users should never use the server Ethernet port (NIC) address since connectivity can be lost if the server is unreachable.

Security certificate requirements:

By default, all Cisco VSM server include a self-signed certificate. Using the self-signed certificate on the Operations Manager server causes a security warning to appear when users log in the Operation Manager. To avoid this, you can create and install a web server certificate for the Operations Manager servers. The certificate must point to the HA virtual IP address and be installed on both Operations Manager servers (Master and Peer) used in the HA configuration.

For more information:

- [Cisco Video Surveillance Operations Manager User Guide](#)
- [Cisco Video Surveillance Management Console Administration Guide](#) for instructions to install the certificate.

Network Time Protocol (NTP) server:

All servers must be configured with the same NTP configuration to ensure the time settings are accurate and identical.

Passwords:

- The Management Console password for Operations Manager each server. This is the `localadmin` password used to access the Cisco VSM Management Console, and is set during the initial server setup.
- The admin password used to access the browser-based Operations Manager interface.
Media Server Redundancy and Failover

Cisco Video Surveillance Media Servers can be configured in a high availability (HA) arrangement that allows a primary server to be paired with additional Failover, Redundant, or Long Term Storage Media Server. These HA servers provide the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.

Review the following topics for more information.

- Understanding Redundant and Failover Servers, page 12-6
- Understanding Media Server Failover, page 12-8
- Requirements, page 12-9
- Failover Server Recommended Load and Limitations, page 12-10

Related Information
- Extending Video Archive Retention Using Long Term Storage Servers, page 10-2

Understanding Redundant and Failover Servers

Table 12-2 describes the different Media Server high availability types.

<table>
<thead>
<tr>
<th>Media Server Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary server</td>
<td>Both streams are sent to the Primary server only</td>
<td>The Primary Media Server processes the camera video feeds, stores and plays back recorded video, among other tasks.</td>
</tr>
</tbody>
</table>

Usage Notes
- All Media Servers are assigned the Primary HA role by default.
- A 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).
- A co-located Media Server is automatically added to the Operations Manager and activated. The default co-located server name is “VsomServer”.

Table 12-2 Redundant and Failover Servers
Redundant server

Stream A to Primary, Stream B to Redundant:

All Streams to Both Servers:

A Redundant Media Server provides additional computing power for the cameras associated with a Primary server.

- Unicast—The camera’s video streams are sent to different servers. For example, stream A is sent to the Primary server, and stream B to the Redundant server. If the Primary server goes down, the video from Stream B is still saved to the Redundant server.

- Multicast—Both camera video streams are simultaneously sent to both servers.

Note  See the “Configuring Multicast Video Streaming” section on page 11-15 for more information.

Usage Notes

- A Redundant Media Server can support multiple Primary servers. You must ensure that the Redundant server contains the disk and processing capacity to support all cameras that send video streams to the server.

- The Record Now feature is not available on redundant servers. The Record Now feature is available on the Primary server, or on the failover server if the Primary is down.

Failover server

A Failover Media Server is a hot standby server that assumes system control if the Primary server fails or goes offline.

Usage Notes

- The Failover server does not provide hot-standby functionality for the Redundant server.

- See the “Understanding Media Server Failover” section on page 12-8 for more information.

<table>
<thead>
<tr>
<th>Media Server Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
</table>
| Redundant server  | ![Redundant server example](image.png) | A Redundant Media Server provides additional computing power for the cameras associated with a Primary server.  
- Unicast—The camera’s video streams are sent to different servers. For example, stream A is sent to the Primary server, and stream B to the Redundant server. If the Primary server goes down, the video from Stream B is still saved to the Redundant server.  
- Multicast—Both camera video streams are simultaneously sent to both servers.  
Note  See the “Configuring Multicast Video Streaming” section on page 11-15 for more information.  
Usage Notes  
- A Redundant Media Server can support multiple Primary servers. You must ensure that the Redundant server contains the disk and processing capacity to support all cameras that send video streams to the server.  
- The Record Now feature is not available on redundant servers. The Record Now feature is available on the Primary server, or on the failover server if the Primary is down. |
| Failover server   | ![Failover server example](image.png) | A Failover Media Server is a hot standby server that assumes system control if the Primary server fails or goes offline.  
Usage Notes  
- The Failover server does not provide hot-standby functionality for the Redundant server.  
- See the “Understanding Media Server Failover” section on page 12-8 for more information. |
Understanding Media Server Failover

When a Failover Media Server is associated with a Primary server, the Failover polls the Primary every two minutes to verify connectivity. If the failover does not receive a response after three successive tries, the Primary is assumed to be down or offline and the Failover assumes the Primary role.

- A few minutes of recording may be lost between the loss of the Primary Media Server and the Failover assuming control.
- A Failover Media Server can only stand in for one Primary server at a time (if a Failover server is already acting as the Primary for a Media Server that is down, the Failover cannot assume control for a second Primary Media Server.
- When the Primary Media Server is down and the Failover has taken over the role of the Primary server, and a DHCP based Medianet discovered camera has a change of IP address, the Cisco VSM Operations Manager will not reconfigure the camera to the new IP address until the Primary Media Server comes back up. This is because Cisco VSM Operations Manager does not allow any configuration changes on the cameras when the Primary server is down.

Failover status is indicated in the server Status page (Figure 12-3). The possible Failover Status values are:

- In Failover
- Not In Failover
- Could Not Failover (this occurs if a different Primary server already failed over to the same Failover server.)

For example, Figure 12-3 displays a Primary Media Server with a critical configuration error that causes a failover.

- The Failover Server status is OK (green), indicating that the server is up and ready to assume control.
- The Failover Status is Failed Over, indicating that a failover occurred.
- The Failover server Status page also displays Failed Over.

**Figure 12-3 Primary and Failover Server Status (in Failover)**
When a user attempts to access live or recorded video from a camera that is associated with the Primary server, the request will time out and be forwarded to the Failover server, which completes the request and sends the requested video.

Because the Failover server maintains the same configuration as the Primary server (in real time), users will not encounter a change in network behavior other than a slight delay while communication is established with the Failover server.

Once the Primary server comes back online, it will automatically resume control from the Failover server. The Failover server will revert to hot standby status.

**Note**
Polling between the servers is coordinated based on the system time in each server. Use a NTP time source to ensure server synchronization.

**Requirements**

Before adding HA Media Servers, verify that the following requirements are met.

**Table 12-3  Requirements**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Requirement Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must belong to a User Group with permissions for <em>Servers &amp; Encoders</em>.</td>
<td>☐</td>
</tr>
<tr>
<td>At least two Media Servers must be enabled:</td>
<td>☐</td>
</tr>
<tr>
<td>• 1 Primary Media Server</td>
<td>☐</td>
</tr>
<tr>
<td>• 1 HA Media Server</td>
<td>☐</td>
</tr>
<tr>
<td>Co-located Servers—The Operations Manager and a single Media Server are enabled on the same server. The following rules apply:</td>
<td>☐</td>
</tr>
<tr>
<td>• The 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).</td>
<td>☐</td>
</tr>
<tr>
<td>• Co-located Media Server cannot be configured with Failover or Redundant Media Servers. Only a long term storage (LTS) server can be associated with a co-located Primary Media Server.</td>
<td>☐</td>
</tr>
<tr>
<td>The time on all servers must be in sync. We recommend using the same network time protocol (NTP) server on all Media Servers to ensure the time settings are accurate and identical.</td>
<td>☐</td>
</tr>
</tbody>
</table>
Determining HA Server Scalability

Before installing and configuring HA Media Servers, determine the number of cameras supported by each primary Media Server, and the number of cameras. See the Cisco Video Surveillance Manager Release 7 Server Performance Guidelines cameras supported in your release.

Although there are no hard limits to the number of cameras that a Primary server or associated HA server can support, the Cisco Video Surveillance Manager Release 7 Server Performance Guidelines provide the recommended maximum number of cameras that can be assigned to a server. We highly recommend that your deployment not exceed these numbers for any server in your deployment.

Failover Server Recommended Load and Limitations

Failover servers can support multiple Primary Media Servers, but can only stand in for one Primary server at a time. Although there are no hard limits to the number of Primary servers that can be associated with a single Failover server, we recommend a maximum of 5 Primary server be associated with a single Failover server. This ratio can be more or less. Design your system so that the Failover Media Servers can handle the potential load.

For example: if 10 Primary Media Server use the same Failover server, you must consider the impact if multiple Primary servers fail. If all 10 Primary Media Servers are critical to your operation, for example, a smaller ratio should be used.

Determining the server loads, ratios and priority is part of the system design and should be planned according to the equipment and needs in your deployment.

Use the following guidelines when determining Failover server deployment:

- A Failover server can only stand in for one Primary server at a time (if a Failover server is already acting as the primary for a Media Server that is down, the Failover cannot assume control for a second Primary Media Server).
- We recommend a maximum of 5 Primary server be associated with a single Failover server. Associating more than 5 Primary servers with a Failover server is not recommended.
- A few minutes of recording may be lost between the loss of the Primary server and the Failover assuming control.
- A 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).
- When the Primary Media Server is down and the Failover has taken over the role of the primary server, and a DHCP based Mediatnet discovered camera has a change of IP address, the Cisco VSM Operations Manager will not reconfigure the camera to the new IP address until the Primary Media Server comes back up. This is because Cisco VSM Operations Manager does not allow any configuration changes on the cameras when the primary server is down.
- Configuration changes cannot be made to the Media Server or associated devices (such as cameras) while the server is in Failover mode. This is because Failover mode is meant as a temporary server to enable continued operations, not as a permanent replacement server.
Designing Virtual Machine Deployment on Cisco UCS Platform Servers and Blades

This guide summarizes high-level design recommendations and best practices for implementing Cisco Video Surveillance on the Cisco Unified Computing System (UCS) B-, C-, E- and Express Series platforms.

Tip

This document includes the following sections:

- Introduction, page 2
- Solution Components, page 4
- Logical Network Topology, page 5
- IP Network Infrastructure, page 6
- Performance and Scalability, page 9
- Storage Considerations, page 9
- Design Recommendations for Deployment Models, page 9
Introduction

This guide summarizes high-level design recommendations and best practices for implementing Cisco Video Surveillance on the following platforms:

- Cisco UCS B- and C- Series platforms
- Cisco UCS Express and E- Series platforms on the Integrated Services Router Generation 2 (ISR G2)

**Note**

This guide does not describe the configuration and operation of the Cisco Video Surveillance (Cisco VSM) products or the deployment of the Cisco VSM virtual machine images on the Cisco UCS platforms. For more information on these subjects, see the “Cisco UCS Platform and VM Documentation” section on page A-5 and the “Cisco Video Surveillance Documentation” section on page A-1.

In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support high-quality IP video surveillance. In other instances, network hardware might require upgrading or reconfiguration to support increased bandwidth needed to support video.

Figure 13-1 represents a virtualized VSM application running on a UCS B- and C- Series platform. 

*Figure 13-1  Cisco IP Video Surveillance on UCS B- and C- Series Platforms*
Figure 13-2 displays the Cisco ISR G2 platform integrating Cisco Video Surveillance on the UCS Express and E-Series platforms. This solution uses a single network access device for remote sites.

Figure 13-2  Cisco ISR G2 With the UCS Express and E-Series Platforms Integrates Video Surveillance on Single Network Access Device for Remote Sites
Solution Components

This guide assumes that the ESXi 5.0 Hypervisor is installed on the UCS server of SRE blade.

The required components for designing and deploying VSM on UCS B-and C-Series platforms include:

- **UCS B- and C-Series servers**—The Cisco UCS Servers can be deployed as rack-mount servers (C-Series) or blade servers (B-Series) running the ESXi 5.0 virtualization software. The B-Series servers deliver a scalable and flexible architecture to meet your data center needs while helping to reduce the total cost of ownership. The C-Series servers address fluctuating workload challenges through a varying balance of processing, memory, I/O, and internal storage resources.

- **UCS Express on a Cisco ISR G2 with SRE 900/910 blade**—The Cisco UCS Express is an SRE blade on an Cisco Integrated Services Routers Generation 2 (ISR G2) branch office router running the SRE-V (ESXi) virtualization software. The 2900 and 3900 series routers have up to four Gigabit Ethernet interfaces onboard, up to four Enhanced High-Speed Wide-Area Network (WAN) Interface Card (EHWIC) interface slots, and up to four service module slots (depending on the model). See the UCS Express Data Sheet for more information.

- **UCS E-Series on a Cisco ISR G2 with E140x or E160x single or double-wide blade**—Cisco UCS E-Series Servers are next-generation power-optimized general-purpose x86 64-bit blade servers designed to be deployed in Cisco ISR G2 branch office router running the SRE-V (ESXi) virtualization software. See the UCS E-Series Data Sheet for a list of the supported single-wide and double-wide blades.

- **Virtualized Video Surveillance Manager (VSM) software**—The VSM software is available as an Open Virtual Appliance (OVA) file on Cisco.com. The OVA package is a tar file with the Open Virtualization Format (OVF) directory inside. Apart from the OVA file, the Video Surveillance Operations Manager (VSOM) virtual machine (VM) License and Video Surveillance Media Server (VSMS) VM License are also required.
  - UCS B-or C-Series: This software runs on a UCS B-or C-Series server in a virtualized environment.
  - UCS Express and E-Series: This software runs on a Cisco ISR series SRE blade in a virtualized environment.

- **Cameras**—The Cisco IP video surveillance camera and analog cameras are attached to encoders, analog gateway network modules for the integrated services router, or third-party IP surveillance cameras.

- **Network**—This component is comprised of the enterprise network—the Media Ready Network. The primary focus of this design guide is to reference the existing design baselines of branch office and wide-area network (WAN) while building on this base of knowledge with IP video Surveillance requirements, best practices, and design recommendations.
Logical Network Topology

Figure 13-3 and Figure 13-4 illustrates the overall logical topology of the networking and video surveillance components, including a UCS B-Series containing the ESXi host running VSM and VSOM, various IP cameras, an external switch, and the operator workstations running the VSOM client.

Figure 13-3  UCS B- and C- Series Logical Network Topology

Figure 13-4  UCS Express and E- Series Logical Network Topology (External or Internal Switch in ISR)
# IP Network Infrastructure

## Table 13-1  IP Network Infrastructure Considerations for VM Deployment

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>More Information/Detailed Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Considerations for the UCS Express</td>
<td>The SRE 900/910 service module must be dedicated to the VSM VM, because the computing requirements for VSM are high. Deploying other VMs on the same SRE 900/910 service module are not recommended and not supported.</td>
<td><a href="#">Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms</a></td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Bandwidth refers to the raw capacity available on a particular transport medium, and is dependent on its physical characteristics and the technology used to detect and transmit signals. The amount of available bandwidth on a network segment directly impacts the quality and performance of the IP Video Surveillance solution and as such should be carefully considered. High-bandwidth, low-delay networks typically do not encounter much performance degradation over time. Low-bandwidth, low-delay networks on the other hand typically experience packet loss due to congestion. High-bandwidth, high-delay networks (so-called Long Fat Networks), such as satellite links, would typically experience significant performance degradation due to the latency.</td>
<td>“Bandwidth” and “Network Performance Considerations” in the <a href="#">Cisco Video Surveillance Solution Reference Network Design Guide</a></td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>QoS refers to the ability of the network to provide special or preferential service to a set of users or applications or both to the detriment of other users or applications or both. Proper design of QoS in an IP Video Surveillance environment is crucial as video transport places unique demands on the network infrastructure to ensure that it is usable, reliable and available to media servers and end-users.</td>
<td>“Quality of Service Considerations” in the <a href="#">Cisco Video Surveillance Solution Reference Network Design Guide</a></td>
</tr>
<tr>
<td>Security</td>
<td>Security focuses on controlling what users have access to a resource while in transit, at the originating node, or when it is processed or stored on a server. One aspect of IP networking is the any-to-any connectivity between networks and users. This strength is also a flaw. There is a certain population of users on the network that must have access to the video surveillance system, but many cannot be trusted to access this data. Video surveillance data is particularly sensitive because access to the system by unscrupulous individuals can expose the enterprise to financial loss and compromise personal safety. This design guide illustrates how to transport video traffic over LAN and WAN with IP security encryption, and also implement administrative controls on who has access to the network.</td>
<td><a href="#">Securing Cisco Video Surveillance Manager, page 3-1</a></td>
</tr>
<tr>
<td>Network Services</td>
<td>One advantage of the any-to-any aspect of IP networks is resource and system access. Examples include the Network Time Protocol (NTP), Dynamic Host Control Protocol (DHCP), Power-over-Ethernet (PoE) and the Cisco Discovery Protocol (CDP) both lower the cost of installation and facilitate troubleshooting.</td>
<td><a href="#">Cisco Video Surveillance Solution Reference Network Design Guide</a></td>
</tr>
</tbody>
</table>
In order to have an effective IP Video Surveillance solution that meets expectations, the video endpoints, server applications, and client endpoints need to be managed on a common network framework, allowing for device and platform health monitoring, fault isolation, and resolution.

Physical security is one component of facilities management in many large organizations. Other components include door access control, which is often closely linked with video surveillance as a key component to the safety and security missions. To achieve the goal of a fully-converged network, the other Building Management Systems (BMSs), such as fire alarms, elevator control (to park elevators in the event of a fire), air quality monitoring (carbon monoxide and smoke detection), and lighting and heating/cooling must be able to communicate with the video surveillance systems.

The first step in achieving this goal is to IP-enable these devices and provide the network infrastructure to support their effective communication between systems. For example, if virtualization is enabled on the IP network to support video surveillance, a practical approach is to also include the BMS devices on the same address space, and in the same network segments, as the video surveillance devices. Typically, the bandwidth requirements of BMSs are very trivial to that of video surveillance, the end users of the data often report to the same organization heads and the likelihood of system integration (now or in the future) is high.
The end goal of migrating from analog-based systems to IP-enabled video surveillance is to move the application from targeting loss prevention, compliance, safety, and security to obtain a greater business value by increasing sales and reducing expenses and exposure to liability. Data mining is the process of detecting some pattern in data. One video surveillance application can be to analyze video feeds to detect certain colors or articles of clothing to identify groups of gang members among patrons at a shopping mall. Video analytics use data mining techniques to detect patterns in data. Video analytics may be performed at the endpoint (IP camera) on specialized digital signal processors (DSPs) by a third-party analytics vendor, or by servers within the enterprise data center. One application of video analytics is to detect the queue length of checkout lines and inform management to increase or decrease the staffing at cash registers to more fully use staff.

In the future, the analysis output of video data can be more economically valuable than the loss prevention role of video surveillance to many retail organizations.

To configure analytic rules on the camera, see the camera product documentation.

To configure the actions that are triggered in Cisco VSM when an analytic event occurs on a camera, see the “Advanced Events” section of the Cisco Video Surveillance Operations Manager User Guide.

### Table 13-1 IP Network Infrastructure Considerations for VM Deployment (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>More Information/Detailed Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Data-Mining and Analytics</td>
<td>The end goal of migrating from analog-based systems to IP-enabled video surveillance is to move the application from targeting loss prevention, compliance, safety, and security to obtain a greater business value by increasing sales and reducing expenses and exposure to liability. Data mining is the process of detecting some pattern in data. One video surveillance application can be to analyze video feeds to detect certain colors or articles of clothing to identify groups of gang members among patrons at a shopping mall. Video analytics use data mining techniques to detect patterns in data. Video analytics may be performed at the endpoint (IP camera) on specialized digital signal processors (DSPs) by a third-party analytics vendor, or by servers within the enterprise data center. One application of video analytics is to detect the queue length of checkout lines and inform management to increase or decrease the staffing at cash registers to more fully use staff. In the future, the analysis output of video data can be more economically valuable than the loss prevention role of video surveillance to many retail organizations.</td>
<td>To configure analytic rules on the camera, see the camera product documentation. To configure the actions that are triggered in Cisco VSM when an analytic event occurs on a camera, see the “Advanced Events” section of the Cisco Video Surveillance Operations Manager User Guide.</td>
</tr>
<tr>
<td>NTP Considerations</td>
<td>NTP must be configured on the VM and ESXi host. Time sync on VMware tools should be disabled on the VM.</td>
<td>Detailed instructions are available in the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.</td>
</tr>
</tbody>
</table>
Performance and Scalability

Refer to the Cisco Video Surveillance Manager Release 7 Server Performance Guidelines for performance and scalability numbers.

Storage Considerations

Media Server VMs running on the UCS platforms support the following storage sources:

- UCS Express and E-Series platforms can access internal storage and iSCSI external storage.
- UCS B- and C- Series platforms can access internal storage, and external storage from Fiber Channel-based SAN storage, such as the Cisco Physical Security Storage System 4RU (CPS-SS: 4-RU) and the Cisco Physical Security Storage System 4RU-EX.

The usable storage is based on the redundant array of independent disks (RAID) level used. For more information, see the following:

Table 13-2 Related Documentation for VM External Storage

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Video Surveillance Storage System documentation</td>
<td>Instructions to install, configure and administer the Cisco Physical Security Storage System.</td>
</tr>
<tr>
<td>Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.</td>
<td>Instructions to associate external storage with a VM running on the Cisco UCS Series platforms, and how to add media partitions to a Cisco VSM VM</td>
</tr>
</tbody>
</table>

Design Recommendations for Deployment Models

A typical IP video surveillance deployment in an enterprise network consists of one or more campus locations running a Cisco Video Surveillance Media Server and a Video Surveillance Operations Manager on an Intel-based Linux Enterprise Server OS (Cisco Physical Security Multiservices Platform or Cisco UCS Platform).

Recommendations

- Deploy Cisco VSM on UCS Express or E-Series platforms only if you plan to record up to 32 streams 1 M or 15 streams @ 2 M or 7 streams @ 4 M.
  - For the UCS Express, consider dedicating the entire SRE 9xx for video surveillance.
  - UCS Express or E-Series platforms are deployed on the Cisco Services Ready Engine (SRE) with ESXi running a video surveillance virtual machine (VM). The VMs can run the Cisco Video Surveillance Media Server and Video Surveillance Operations Manager software.
- Locations with more than 32 video surveillance cameras can be deployed on standalone hardware or the UCS C-Series server running a video surveillance virtual image.
- For enterprise-level deployments, we recommend to use the UCS B-Series servers in the data center.
- In cases where implementing cameras is the only requirement, it may be practical to transport the camera feeds across the WAN for archiving. However, in most deployments, local storage is necessary due to the bandwidth required and the bandwidth costs.
• A typical enterprise deployment consists of one or more campus locations running the Cisco Video Surveillance Media Server.
• Branch offices and teleworker locations may view and administer the video surveillance system
• External users and external organizations can also access the system using an Extranet or the public Internet and a web browser.

Figure 13-5 illustrates the topology and application services deployed in an enterprise-wide implementation of IP-based video surveillance.

The branch locations are connected to the enterprise campus by WAN technologies, including Metro Ethernet, private line, the public Internet, or a Layer-2 or Layer-3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) deployment. With a Layer-2 MPLS deployments (Pseudowire), IP cameras can be Ethernet-attached to a remote switch and can transport images through the carrier network, provisioned and managed by the Video Surveillance Operations Manager, either at a branch location or a central location. Branches attached through a Layer-3 MPLS network, leased line, or over the Internet can support viewing stations and IP cameras that can be managed by either the campus or branch deployment.

Cisco technologies, such as Dynamic Multipoint Virtual Private Network (DMVPN), can be overlaid on to the WAN transport to provide data privacy and authentication by way of IP security (IPsec) encryption. To ensure the prioritization of voice, video, and mission-critical applications over the WAN, QoS is deployed on the WAN. Where multiple WAN links exist, Performance Routing (PfR) can be
enabled to provide intelligent path selection and the ability to route around brownouts and transient failures, thereby enhancing what can be provided by traditional routing protocols, such as the Enhanced Internal Gateway Routing Protocol (EIGRP).

The decision as to whether a specific environment should implement the Cisco Video Surveillance on UCS Express or E-Series platforms at a branch location and archive data at the branch—or provision cameras off the campus implementation of the Cisco Video Surveillance Manager—depends on the number of cameras, the resolution, frame or bit rate of the camera, quality factors of the cameras, and the bandwidth cost and availability at the remote locations.
WAN Considerations

WAN is used to connect different LANs and typically includes a broad geographic area. WAN services are leased from service providers who provide different speeds and connectivity options. Figure 13-6 illustrates how a remote branch office relies on the connectivity provided by a WAN service provider.

![Figure 13-6 Service Provider Network](image)

Deploying a video surveillance solution through a WAN environment presents challenges that are not typically seen in a LAN. In a LAN environment, it is common to see 1 Gbps and 10 Gbps of bandwidth, while in a WAN environment, most connections are less than 10 Mbps; many remote connections operate on a single T1 (1.544 Mbps) or less.

These inherent bandwidth constraints require careful evaluation of the placement of cameras and Media Servers, and how many viewers can be supported at remote sites simultaneously. By using child proxies, bandwidth requirements can be reduced to transport video streams across WAN connections.

The placement of recording devices also becomes important. The video can be streamed to a central site using lower frame rates or resolution, but another attractive alternative is to deploy Media Servers at the remote sites and stream the traffic using the LAN connectivity within the remote site.

A point-to-point or leased line is a link from a primary site to a remote site using a connection through a carrier network. The link is considered private and is used exclusively by the customer. The circuit usually is priced based on the distance and bandwidth requirements of the connected sites.

Technologies, such as Multilink Point-to-Point Protocol (PPP), allow several links to be bundled to appear as a single link to upper routing protocols. In this configuration, several links can aggregate their bandwidth and be managed with only one network address. Because video surveillance traffic requirements tend to be larger than other IP voice and data applications, this feature is attractive for video surveillance applications.

Hub-and-spoke, also known as star topology, relies on a central site router that acts as the connection for other remote sites. Frame Relay uses a hub-and-spoke topology predominantly due to its cost benefits, but other technologies, such as Multiprotocol Label Switching (MPLS), have mostly displaced Frame Relay.
Example 1—Network Bandwidth Usage

Figure 13-7 and Figure 13-8 illustrate a simple scenario with two sites. Each site has a Media Server and each is the direct proxy for an IP camera. Three video monitoring workstations are active in Site A and each IP camera generates 1 Mbps of network traffic.

Two monitoring workstations display video streams from Camera 1 and Camera 2, while one monitoring workstation displays three video streams: two streams from Camera 1 and one stream from Camera 2. The network bandwidth required to display video streams for Camera 2 in Site A is relatively small for a LAN environment, but the traffic from Camera 1 can be significant for WAN environments because four different 1 Mbps streams must traverse the WAN locations.

Note

For simplicity, the Operations Manager has been removed from Figure 13-7 and Figure 13-8.
Design Recommendations for Deployment Models

Figure 13-8  UCS Express and E- Series: Network Bandwidth Requirements
Example 2—Sites with Remote Storage

Figure 13-9 and Figure 13-10 display how Media Servers can be deployed at different WAN locations to minimize the bandwidth requirements. By deploying the Media Servers close to viewers and edge devices, the network traffic remains local to each site. Archiving video streams at each location is also an attractive solution to minimize the network traffic between sites.

In this example, Site A and Site C have Media Servers acting as direct proxies and archives for the IP cameras. Because both sites archive and distribute video to the monitoring workstations locally, the network traffic remains local to each site.

Site B can function without a local Media Server, but all video streams must traverse the WAN connections. Because Media Server A is the direct proxy for Camera B, the 1 Mbps stream must reach Media Server A before reaching any monitoring workstation. A total of 3 Mbps would be required for both monitoring workstations in Site B to receive video from Camera B.

Figure 13-9  UCS B- and C- Series: Sites with Remote Storage
Figure 13-10  UCS Express and E-Series: Sites with Remote Storage
Example 3—Distributed Media Servers

Figure 13-11 and Figure 13-12 display a deployment with several remote sites, each with a local Media Server acting as the direct proxy and archive for local IP cameras. In this scenario, all recording occurs at the remote sites and live video streams are viewed by OM viewers and VM monitors (video walls) at the headquarters.

The Media Server at the headquarters could also have Parent-Child proxies to each remote Media Server and request the remote streams only when required at the headquarters. This would have less bandwidth impact when the same stream is requested by more than one viewer because the traffic would be contained locally in the headquarters LAN.
Design Recommendations for Deployment Models

Chapter 13      Designing Virtual Machine Deployment on Cisco UCS Platform Servers and Blades

Figure 13-12  UCS Express and E-Series: Distributed Media Servers

- Site A: Video Streams from Site A to Media Server, then to SRE.
- Site B: Video Streams from Site B to Media Server, then to SRE.
- Site C: Video Streams from Site C to Media Server, then to SRE.
- Site D: Video Streams from Site D to Media Server, then to SRE.
- Headquarters: Operations Manager connected to Media Server, Storage Server, and Monitoring Workstation.
- Video Streams from Headquarters to Media Server, then to SRE.
High Availability

See the “Server High Availability” section on page 12-1 for more information.
PART 6

Camera Discovery and Bulk Deployment
Bulk Camera Configuration and Deployment

- Adding Multiple Cameras, page 14-1
- Applying Camera Settings to Multiple Cameras, page 14-3

Adding Multiple Cameras

Although cameras can be added individually, you can also deploy multiple cameras using one of the following methods.

- Importing Cameras from a List, page 14-1
- Discovering Cameras on the Network, page 14-3

Importing Cameras from a List

Multiple cameras or encoders can be imported using a comma separated value (CSV) file that includes configuration details for each device (Figure 14-1). This same method can be used to update existing camera configurations.

Figure 14-1 summarizes the process to import devices from a CSV file. Devices can be added in Enabled state if all required configurations are included, or in Pre-Provisioned state if configurations are missing or if the devices are not yet available on the network. If an error occurs, correct the CSV file and try again.

See the Cisco Video Surveillance Operations Manager User Guide for instructions to create and import the CSV file.
Best Practices

- Cameras, encoders and servers can be pre-provisioned in Release 7.2 and higher.
- Pre-provisioned devices are devices waiting to be added to Cisco VSM. You can make additional configuration changes, but the device cannot stream or record video until the configuration and network issues are resolved. Choose Enable from the Device Settings menu to enable the device video functions.
- If the CSV file details are accurate and complete, the devices are added to Cisco VSM and video from the cameras is available for viewing and recording.
- If any required fields are left blank, or if any devices in the file are not available on the network, then the devices are added to Cisco VSM in pre-provisioned state, even if the pre-provisioned option is deselected. Complete the configuration to change the status to Enabled.
- If any fields are inconsistent with the Cisco VSM configuration, the import action fails and an error file is created that specifies the problem(s). For example, if the CSV file specifies a Media Server or location that does not exist in your Cisco VSM configuration, an error occurs. Correct the CSV file and try again.
- You cannot mix device types in the import file. For example, the file can include servers, encoders, IP cameras, or analog cameras only.
• To update existing cameras, use the Camera Report to create a spreadsheet with camera details. Then modify the sheet for your cameras.

Discovering Cameras on the Network

Cameras can be discovered when they are added to the network, and automatically added to the Cisco VSM configuration. The camera configuration can include a camera template and additional camera settings.

Refer to the following for more information:
• Discovering Cameras on the Network, page 15-1
• Applying Camera Settings to Multiple Cameras, page 14-3

Applying Camera Settings to Multiple Cameras

Camera settings can be applied to multiple cameras using the following methods:

<p>| Table 14-1 Camera Bulk Configuration Options |  |</p>
<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Description</th>
<th>When to Apply</th>
</tr>
</thead>
</table>
| Camera Templates | Templates simplify camera configuration by defining the image quality, recording schedule, event triggered actions, alerts, and other attributes used by a set of cameras. | • When the camera is added to Cisco VSM  
• To change the basic settings for a group of cameras |
| Pre-Defined Camera Settings | Camera settings are the device-specific settings that are not included in the camera templates. For example, motion detection configuration, camera tamper settings, NTP and timezone settings are all configured on each individual device. | You can select the Camera Setting when adding a camera manually, when the device is discovered on the network, or when adding multiple devices using a CSV file. If the cameras are already added to Cisco VSM, use Bulk Actions to apply the Camera Settings to multiple devices. |
| Camera Bulk Configuration | Bulk Actions allows you to change the configuration or take actions for multiple cameras. For example, you can enable, disable, or delete the devices. You can also change the template, repair the configurations, change the location or change the password used to access the device. | Click Bulk Actions (under the Cameras tab) to apply changes to multiple existing cameras |
| Importing changes from a CSV file | Import a CSV file with existing cameras to update the configuration for those devices. | Use the Camera Report to create a spreadsheet with camera details. Then modify the sheet for your cameras. |

Note

See the Cisco Video Surveillance Operations Manager User Guide for instructions to use each of these features.
Discovering Cameras on the Network

Although IP cameras can be manually added to Cisco VSM, cameras can also be discovered on the network and automatically added to the Cisco VSM configuration.

Refer to the following topics for more information:
- Camera Discovery Options, page 15-2
- Understanding Camera Conflicts During Discovery, page 15-3
- Enabling the Auto Configuration Defaults for a Camera Model, page 15-4
- Discovering Non-Medianet Cameras Using Bonjour, page 15-5
- Cameras Pending Approval List, page 15-7
- Discovering Medianet-Enabled Cameras, page 15-8
  - Medianet Requirements, page 15-8
  - Medianet Overview, page 15-10
  - Configuring a DHCP Server with Option 125, page 15-12
  - Medianet Camera Discovery Procedure, page 15-13
  - High Availability Impact on Medianet Cameras, page 15-14

Related Documentation
- Understanding Device Conflicts, page 8-7
- Cameras can be installed in the same network (NAT) as the Cisco Media Server that supports them, or in a different network. See Adding Cameras From Different Networks (NATs), page 8-11 for more information.
Camera Discovery Options

Cisco VSM can discover network cameras that are added to the network using one of the following methods:

<table>
<thead>
<tr>
<th>Discovery Method</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Discovery</td>
<td>Medianet-enabled cameras can be discovered automatically and added to Cisco VSM (when added to the network).</td>
<td>Discovering Medianet-Enabled Cameras, page 15-8</td>
</tr>
<tr>
<td>Note</td>
<td>Medianet cameras must be configured with an admin user.</td>
<td></td>
</tr>
<tr>
<td>Manually Trigger</td>
<td>Cameras that do not support Medianet can still be discovered on the network, but the discovery must be manually triggered and the cameras must support the Bonjour discovery feature.</td>
<td>Discovering Non-Medianet Cameras Using Bonjour, page 15-5</td>
</tr>
<tr>
<td>Tip</td>
<td>Enable “Bonjour” on the cameras using the camera UI. For example, Cisco 3xxx,6xxx, and 7xxx cameras. See the camera documentation for more information.</td>
<td>Documentation for the camera(s) to be discovered</td>
</tr>
</tbody>
</table>

Auto-Configuration Default Configuration

If the Auto-configuration default option is enabled for a camera model, then the basic configuration, camera settings, and camera template is automatically applied to the camera, and the camera is added directly to the enabled state (Figure 15-1). Auto-configuration default settings are accessed in the System Settings page. See the “Enabling the Auto Configuration Defaults for a Camera Model” section on page 15-4 for more information.

Cameras Pending Approval List

If the Auto-configuration default option is disabled for a camera model, then the cameras are added to the Cameras Pending Approval list (Figure 15-1). This allows you to review the discovered cameras, add additional configuration settings if necessary, and manually approve the camera so it can be added to Cisco VSM. See the “Cameras Pending Approval List” section on page 15-7 for more information.

Supported Cameras

To view the camera models that support discovery, open the Auto Configuration Settings page and click on a camera manufacturer. See the Enabling the Auto Configuration Defaults for a Camera Model, page 15-4.
Understanding Camera Conflicts During Discovery

Cameras are identified in Cisco VSM discovery by the device IP Address, and serial number, mac address/hardware ID. If a camera is discovered with values in these fields that already exist in the Cisco VSM configuration, the camera records will either be merged, or placed in a collision state.

See Camera Discovery and IP Addresses Conflicts, page 8-14 for more information.
Enabling the Auto Configuration Defaults for a Camera Model

Enable the auto-configuration default settings to automatically apply a set of basic configurations to cameras that are discovered on the network.

Auto-configuration is disabled for all camera models by default. You must enable the defaults for each camera model.

**Figure 15-2 Device Auto Configuration**

**Usage Notes**

- If auto-configuration is not enabled for a camera model (or if the auto-configuration fails) then the camera is placed in the *Cameras Pending Approval* list. See the “Cameras Pending Approval List” section on page 15-7 for more information.
- If the auto-configuration fails, cameras can also be placed *Enabled:Critical* state. For example, if the entered password does not match the password configured on the device.
- Medianet-enabled devices also include an *Uninitialized* option. Select this to log in to the camera using the default device credentials. Enter a password to automatically replace the device password with the new setting (the username is read-only).
Discovering Non-Medianet Cameras Using Bonjour

Cameras that do not support Medianet can still be discovered on the network, but the discovery must be manually triggered. The cameras must also support the Bonjour discovery feature, and Bonjour must be enabled on the device. To enable Bonjour on cameras using the camera UI (for example, Cisco 3xxx, 6xxx, and 7xxx cameras), see the camera documentation.

You can also (optionally) enable the auto-configuration defaults for the camera model to automatically complete the basic camera properties and enable the camera in Cisco VSM.

Procedure

<table>
<thead>
<tr>
<th>Table 15-2</th>
<th>Manual Camera Discovery Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Add additional camera licenses for non-Cisco cameras, if necessary.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>Review the overview sections to understand the discovery process.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Discovering Non-Medianet Cameras Using Bonjour

Table 15-2  Manual Camera Discovery Steps (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enable the Bonjour discovery feature on each camera, if not enabled by default. See the product documentation for the device to determine Bonjour support and configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>(Optional) Enable auto-configuration presets. If auto-configuration is enabled for the camera model, the camera will automatically be added to Cisco VSM. See the Cisco Video Surveillance Operations Manager User Guide for instructions.</td>
</tr>
</tbody>
</table>
| Step 4 | Trigger the discovery process See the Cisco Video Surveillance Operations Manager User Guide for instructions.  
 a. Click Cameras.  
b. Choose Add > Discover New Cameras. |
| Step 5 | Wait for the camera to be discovered and be added to the Operations Manager. 
  - Discovery can take a few minutes based on the factors such as the camera configuration, availability of the Media Servers, and other variables.  
  - If a discovered camera has the same device ID fields as an existing camera entry (IP Address, and serial number, mac address/hardware ID), then the records are either merged, or placed in conflict. See Understanding Camera Conflicts During Discovery for more information. |
| Step 6 | Approve cameras that were added to the Cameras Pending Approval list. If auto-configuration is not enabled for the camera model, the camera is added to the Cameras Pending Approval list, which allows you to apply additional configurations and approve (add) the camera. See the “Cameras Pending Approval List” section on page 15-7 for more information  
| Step 7 | Complete the camera configuration. If auto-configuration was enabled for the camera, edit the camera settings if necessary. See the Cisco Video Surveillance Operations Manager User Guide for instructions. |
Cameras Pending Approval List

Discovered cameras that are not auto-configured are held in the Cameras Pending Approval list so they can be reviewed and updated before being added to Cisco VSM (Figure 15-4). The cameras in this list are not available for streaming or recording video.

These cameras can also be added to the blacklist which deletes them from the Cisco VSM configuration and prevents them from being found in future discovery operations.

Figure 15-4  Cameras Pending Approval

Camera models that have the auto-configuration defaults enabled are added to Cisco VSM. If auto-configuration fails or is not enabled, the camera is added to Cameras Pending Approval. If the camera is in Enabled: Warning or Critical state, go to device Status page to get information, fix the problem and choose Repair Configuration from the Device Settings menu.

Procedure
To move cameras from the Cameras Pending Approval list to either Cisco VSM or to the blacklist, refer to the Cisco Video Surveillance Operations Manager User Guide for instructions.
Discovering Medianet-Enabled Cameras

Network (IP) cameras that support Cisco Medianet can be automatically discovered when they are added to the network. Cameras can also be discovered by a Media Server configured in a different subnet.

Refer to the following topics for more information:
- Medianet Requirements, page 15-8
- Medianet Overview, page 15-10
- Configuring a DHCP Server with Option 125, page 15-12
- Medianet Camera Discovery Procedure, page 15-13
- High Availability Impact on Medianet Cameras, page 15-14

Medianet Requirements

For cameras to be automatically discovered on the network using Medianet, the following requirements must be met:

<table>
<thead>
<tr>
<th>Table 15-3 Medianet Discovery Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements</strong></td>
</tr>
<tr>
<td>The network (IP) camera must support Cisco Medianet.</td>
</tr>
<tr>
<td>• Medianet cameras must be configured for DHCP (cameras that do not support Medianet can only be added using a static IP address).</td>
</tr>
<tr>
<td>• See the camera documentation for information.</td>
</tr>
<tr>
<td>• Examples of Medianet cameras include the Cisco models 4300, 4300E, 4500, 4500E and 26xx.</td>
</tr>
<tr>
<td>• See the Release Notes for Cisco Video Surveillance Manager, Release 7.7 for a summary of supported Cisco cameras and required firmware. See also the camera product information at <a href="http://www.cisco.com/go/physicalsecurity">http://www.cisco.com/go/physicalsecurity</a> (click View All Products, and select the camera model under Video Surveillance IP Cameras).</td>
</tr>
</tbody>
</table>
Discovering Medianet-Enabled Cameras

The camera must be able to discover an available Media Server using one of the following methods:

- The camera’s “Preferred Media Server List” is enabled using the camera UI. This list is also configured with up to four Media Server IP addresses.
- A Cisco IOS DHCP server must be installed and configured with Option 125 to return a list of Media Server IP addresses. See the “Configuring a DHCP Server with Option 125” section on page 15-12 for instructions.

If both of these options are enabled, the manually-entered “Preferred Media Server List” is used by the camera. If the list is disabled or empty, DHCP is used.

If neither of these options is enabled, auto-discovery will fail.

Related Information

- Camera user documentation
- Cisco Medianet FAQ
- Medianet Reference Guide

A functioning Cisco VSM 7.x system must be installed and configured on the network. See the following for more information:

- Cisco Video Surveillance Manager: Install and Upgrade Guide
- Cisco Video Surveillance Operations Manager User Guide
- Cisco Video Surveillance 7 Documentation Roadmap
Medianet Overview

To enable Medianet discovery, you must install a Medianet-enabled IP camera on the network, as shown in Figure 15-5. A Cisco IOS DHCP server must also be installed and configured with Option 125 to provide a list of up to 16 Media Server IP addresses.

Summary Process

**Figure 15-5  Medianet Camera Discovery Summary**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Media Server is discovered</td>
</tr>
<tr>
<td></td>
<td>The camera discovers a valid Media Server IP address using one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Camera’s “Preferred Media Server List”</strong>—The camera UI is populated with up to 4 Media Server IP addresses.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP</strong>—A DHCP request returns the camera IP address and list of up to 16 Media Server IP addresses.</td>
</tr>
<tr>
<td></td>
<td>In each method, the list of Media Server IP addresses are polled in order until the request is accepted.</td>
</tr>
<tr>
<td></td>
<td>If both of these options are enabled, the manually-entered “Preferred Media Server List” is used by the camera.</td>
</tr>
<tr>
<td></td>
<td>If neither of these options is enabled, auto-discovery will fail.</td>
</tr>
</tbody>
</table>
**Discovering Medianet-Enabled Cameras**

**Detailed Process**

**Note** When the camera is added to the network, it contacts the DHCP server, which returns the camera network settings (including IP address). Medianet cameras are factory-configured for DHCP by default. If the camera IP address is set to static, then the DHCP address is ignored (released).

**Step 1**

The IP camera attempts to connect to a Cisco VSM Media Server using one of the following methods:

- The camera UI is configured with up to four Media Server IP addresses (in the “Preferred Media Server List”).
- A DHCP server configured with Option 125 provides a list of MS IP addresses (see attached from the VSOM user guide).

The IP camera attempts to connect to the Cisco Media Servers (in order of the IP addresses). If a Media Server does not reply, then the camera attempts to connect to the next server in the list.

**Note** The camera first tries to connect to any Media Server addresses that were manually entered on the camera. If there are no manual entries, or if none of the manually-entered Media Servers accepts the connection request, then the camera attempts to connect to the Media Server addresses sent by the DHCP server. If neither of these options is enabled, auto-discovery will fail.

**Step 2**

When the camera connects to a Media Server, the camera is also added to the Operations Manager configuration.

- If Auto-Configuration is enabled for the camera model, the configuration settings (including a static IP address) are applied and the camera is placed in Enabled state. The configuration includes a camera template, Location, and permanent Media Server assignment. See the “Enabling the Auto Configuration Defaults for a Camera Model” section on page 15-4.
- If the Auto-Configuration is disabled (default), then the camera is placed in the Cameras Pending Approval list. See the “Cameras Pending Approval List” section on page 15-7.

**Note** When the camera configuration is applied, the IP address provided by the DHCP server is retained. You can change the IP address using the camera configuration page, if necessary.

**Step 3**

After the camera is added to Cisco VSM, use the Operations Manager to complete the device configuration:

- If the Auto-Config settings were applied (and camera is placed in Enabled state), revise the camera settings if necessary.
- If the camera was added to the Pending Approval list, complete the required config and approve the camera.
Step 3  Once the camera is added to the Operations Manager, you can apply additional configurations, or approve the camera (if it was added to the Cameras Pending Approval list).

Configuring a DHCP Server with Option 125

Complete the following procedure to configure the DHCP Option 125 on a Cisco IOS device. This is required to support Cisco VSM Medianet-enabled camera auto-discovery.

Procedure

Note  Only Cisco IOS DHCP servers are supported for Option 125 to support Medianet camera discovery.

Step 1  Convert the Media Server IP address to a HEX value.
  - The Media Server IP address is the server that the Medianet camera will register with.
  - The HEX value is used in the DHCP server Option 125 configuration.
    
a.  Search for an online tool that can be used to convert the Media Server IP address to HEX.
    - For example, search for “IP to HEX Converter” tools.
  b.  Convert the camera’s IP address to HEX:
    - For example, covert the Media Server IP address 10.194.31.1 to the HEX value 0AC21F01.

Step 2  Add additional HEX values to the Media Server HEX value, as required by your DHCP server.

Note  Each DHCP server may require additional HEX strings to be added before and after the Media Server HEX value. This entire HEX string is entered in the DHCP Option 125 configuration. Be sure to use the correct HEX format, as defined in your DHCP server documentation.

For example, a Cisco IOS DHCP server requires that the following HEX values be added before and after the Media Server HEX value:

a.  Prefix the following value to the Media Server HEX:
    0000.0009.0b14.0901.

b.  Append the following value to the Media Server HEX:
    .0050.0001

The complete HEX string used in the DHCP server Option 125 configuration (for Cisco IOS devices) is:

0000.0009.0b14.0901. 0AC21F01.0050.0001

Step 3  Configure the Cisco IOS DHCP server to advertise Option 125 to the endpoints.

For example:

ip dhcp pool MYADDRESSPOOL
    network 10.194.31.0 255.255.255.0
    option 125 hex 0000.0009.0b14.0901. 0AC21F01.0050.0001
    default-router 10.194.31.254
Discovering Medianet-Enabled Cameras

Note 0AC21F01 is the HEX value of the converted Media Server IP address. The entire required HEX value is 0000.0009.0b14.0901. 0AC21F01.0050.0001.

Note Other DHCP servers may require a different format for the HEX value such as prefixing x to the values or prefixing a \. See your DHCP server documentation for more information.

Medianet Camera Discovery Procedure

Complete the following procedures to discover new Medianet cameras.

**Table 15-4  Summary Steps: Camera Discovery**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description and more information</th>
</tr>
</thead>
</table>
| Step 1  Verify that the Medianet Requirements are met. | Medianet Requirements, page 15-8  
You must have:  
- A Medianet-enabled IP camera configured with DHCP.  
- At least one Media Server and Operations Manager.  
- A DHCP server configured with Option 125 to provide Media Server IP addresses to the camera during discovery. See the “Configuring a DHCP Server with Option 125” section on page 15-12 for instructions.  
Note Cameras that do not support Medianet can only be added using a static IP address. |
| Step 2  Review the overview sections to understand the discovery process. | Review the following topics to understand the discovery and auto-configuration process.  
- Camera Discovery Options, page 15-2  
- Discovering Medianet-Enabled Cameras, page 15-8 |
| Step 3  Install a Medianet network camera and use the camera configuration UI to enable DHCP and add an admin user (if necessary). |  
- Cisco network cameras (such as the Cisco 26xx series) have Medianet and DHCP enabled by default.  
- If a static IP addresses is configured on the camera, or if a list of Media Server IP addresses is configured on the camera, then those values configured on the camera are used and the DHCP settings are ignored. See the camera documentation for more information. |
| Step 4  (Optional) Enable auto-configuration presets. | If auto-configuration is enabled for the camera model, the camera will automatically be added to Cisco VSM.  
Enabling the Auto Configuration Defaults for a Camera Model, page 15-4 |
### Table 15-4  Summary Steps: Camera Discovery (continued)

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Task</th>
<th>Description and more information</th>
</tr>
</thead>
</table>
|        | Wait for the camera to be discovered and be added to the Operations Manager. | • Discovery can take a few minutes based on the factors such as the camera configuration, availability of the Media Servers, and other variables.  
  • If a discovered camera has the same device ID fields as an existing camera entry (IP Address, and serial number, mac address/hardware ID), then the records are either merged, or placed in conflict. See Understanding Camera Conflicts During Discovery for more information. |

| Step 6 | Approve cameras that were added to the Cameras Pending Approval list. | If auto-configuration is not enabled for the camera model, the camera is added to the Cameras Pending Approval list, which allows you to apply additional configurations and approve (add) the camera.  
Open the Cameras Pending Approval list to modify the camera configuration and either approve the camera or move it to the blacklist.  
See the “Cameras Pending Approval List” section on page 15-7 for more information |

| Step 7 | Perform additional configuration, if necessary | See the Cisco Video Surveillance Operations Manager User Guide for more information. |

### High Availability Impact on Medianet Cameras

When the Primary Media Server is down and the Failover has taken over the role of the Primary server, and a DHCP based Medianet discovered camera has a change of IP address, the Cisco VSM Operations Manager will not reconfigure the camera to the new IP address until the Primary Media Server comes back up. This is because Cisco VSM Operations Manager does not allow any configuration changes on the cameras when the Primary server is down.
PART 7

User Access
User access to Cisco VSM video is controlled by the user account access permissions, and the locations to which cameras and other resources are assigned.

For example, a user account is assigned to one or more user groups. Those user groups provide access to the cameras and resources for a location (and its sub-locations), such as campus A, or Building 1. In addition, each user group is associated with a user Role that defines access permissions for viewing video and managing the system.

Cameras and other resources are also assigned to a location. Users can only access the video, devices, and resources for the locations they belong to.

Refer to the following topics for more information:

- Understanding User Access Permissions, page 16-2
- Create a User Access Plan, page 16-3
- Understanding the Impact of a User’s Location, page 16-3
  - Understanding the System-Defined User Roles, Groups and Accounts, page 16-5
  - Understanding Permissions, page 16-6
  - Understanding the Super Admin, page 16-9
  - Understanding Dual Login, page 16-10
- Provide Access from an LDAP Server (Active Directory), page 16-10

Related Information

- Using Locations to Limit User Access, page 17-1
Understanding User Access Permissions

Add user accounts to Cisco Video Surveillance Operations Manager to provide access to both the browser-based Operations Manager and the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application.

Video and system access is based on the following:

- The user group(s) to which the user is assigned: user groups are associated with a user Role, which defines the access permissions for the group.
- The location assigned to the user group(s). Users can only access the devices and video for that location (and its sub-locations).
- Users can be assigned to multiple user groups, and gain the combined access permissions for all groups.

For example, Figure 16-1 summarizes the user Roles, groups and user accounts that must be configured for user access.

![Figure 16-1 Users, User Groups, and Roles](image)

Roles define the access permissions for different types of users. For example, create an **operator** Role that allows users to view live and recorded video, and an **administrator** Role that allows users to configure cameras and add new users.

When the Roles are assigned to a user group, any user added to that group will inherit the Role permissions. Users also gain access to different types of resources based on the user group location.

For example, create an **Operator** Role that allows users to view video, but does not allow configuration of cameras or other system resources. When you add that Role to a user group, any user added to the group will inherit the Role permissions. In addition, users can access the devices at the group location (including sub-locations), and the templates, schedules and other resources for any location in the same location tree.
Understanding the Impact of a User’s Location

The access permissions for a user are determined by the user group(s) to which they belong, and the location(s) of those groups. For example, a user assigned to a user group at the root location will have access to all cameras and video. A user assigned to a user group at a sub-location, such as a campus, will have access only to the cameras and video at that sub-location.

In the following example, an admin might have access to the root location, enabling him to access all cameras and resources in the system. A guard might only have access to a specific region, allowing him to view video only for that sub-location and its children.

Create a User Access Plan

Create a summary of the User permissions and locations for your deployment, similar to the example in Table 16-1. Your summary should include the User Groups and associated Roles and locations. Also include the user names that will be assigned to each user group.

1. Before you begin, create the location hierarchy as described in Using Locations to Limit User Access, page 17-1.
2. Create the Roles that define access permissions for operators, administrators, and other user types.
3. Create the user groups and assign a Role to each group.
4. Create the user accounts and assign each account to at least one user group. Users assigned to multiple user groups inherit the permissions and locations for all groups.
5. (Optional) Require a second user (such as a manager) to enter their credentials when a user logs in. See the “Understanding Dual Login” section on page 16-10.
6. (Optional) Provide access to users on an LDAP server. See Provide Access from an LDAP Server (Active Directory), page 16-10.

Table 16-1  Sample Roles in a Cisco Video Surveillance Deployment

<table>
<thead>
<tr>
<th>User Group</th>
<th>Role Permissions</th>
<th>Location</th>
<th>User name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guard</td>
<td>View Live Video, View Recordings, Listen to Audio, Export Recordings, Perform PTZ</td>
<td>Building 1</td>
<td>John Smith</td>
</tr>
<tr>
<td>Area Admin</td>
<td>View Live Video, View Recordings, Export Recordings, Perform PTZ, Manage Cameras, Manage Servers and Encoders</td>
<td>Campus 1</td>
<td>Debbie Sanchez</td>
</tr>
<tr>
<td>Admin</td>
<td>View Live Video, View Recordings, Export Recordings, Perform PTZ, Manage Users &amp; Roles, Manage Cameras, Manage Servers and Encoders, Manage Templates, Manage Schedules, Manage Location and Maps, Manage System Settings</td>
<td>System (root)</td>
<td>Krishna Bangalore</td>
</tr>
</tbody>
</table>
More Information

Review the following topics for more information.

- Understanding the System-Defined User Roles, Groups and Accounts, page 16-5
- Understanding Permissions, page 16-6
- Understanding the Super Admin, page 16-9
- Understanding Dual Login, page 16-10
- Provide Access from an LDAP Server (Active Directory), page 16-10

Understanding the System-Defined User Roles, Groups and Accounts

By default, Cisco VSM includes system-defined Roles, groups and users to aid in the initial configuration (see Table 16-2). System-defined Roles, groups and users cannot be updated or deleted.

Table 16-2  System-Defined User Roles, Groups and Accounts

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles</td>
<td>• super_admin_role—includes all management and operation access permissions.</td>
</tr>
<tr>
<td></td>
<td>• local_admin_role—provides all operator functions, but limited and</td>
</tr>
<tr>
<td></td>
<td>commonly used management tasks such as managing cameras, Media</td>
</tr>
<tr>
<td></td>
<td>Servers, encoders, Video Walls, locations &amp; maps, views and alerts.</td>
</tr>
<tr>
<td></td>
<td>• operator_role—provides all operator permissions.</td>
</tr>
<tr>
<td>User Groups</td>
<td>• super_admins—assigned the super_admin_role.</td>
</tr>
<tr>
<td></td>
<td>• operators—assigned the operator_role.</td>
</tr>
<tr>
<td>Users</td>
<td>• admin—assigned to the super_admins user group, which gives the user</td>
</tr>
<tr>
<td></td>
<td>super_admin_role permissions. The admin is a root system user and</td>
</tr>
<tr>
<td></td>
<td>cannot be modified or deleted. The default admin username and password is</td>
</tr>
<tr>
<td></td>
<td>admin/admin.</td>
</tr>
<tr>
<td>Note</td>
<td>A super-admin is anybody that has all permissions at the root location.</td>
</tr>
<tr>
<td></td>
<td>• operator—assigned to the operators user group, which gives the user</td>
</tr>
<tr>
<td></td>
<td>operator_role permissions. The default username and password is</td>
</tr>
<tr>
<td></td>
<td>operator/operator.</td>
</tr>
<tr>
<td>Note</td>
<td>A local-admin user account is not included by default. You must add a</td>
</tr>
<tr>
<td></td>
<td>user and add them to a user group associated with the</td>
</tr>
<tr>
<td></td>
<td>local_admin_role, if necessary.</td>
</tr>
<tr>
<td>LDAP Users</td>
<td>Members of an external Lightweight Directory Access Protocol (LDAP) Active</td>
</tr>
<tr>
<td></td>
<td>Directory user database can be granted access to Cisco VSM. See the</td>
</tr>
<tr>
<td></td>
<td>Provide Access from an LDAP Server (Active Directory), page 16-10 for more</td>
</tr>
<tr>
<td></td>
<td>information.</td>
</tr>
</tbody>
</table>
Understanding Permissions

A user’s access permissions are defined by the user group that the user belongs to and the Role associated with that user group. The user group also determines the location that a user has access to. The user’s access permissions are for that location only.

User Roles define the permissions that are assigned to a user group. Click the Roles tab to view or modify the permissions that can be assigned to a Role (Figure 16-3). Permissions are divided into two categories: Manage and Operate. Select or de-select the check boxes to add or remove permissions.

Default Roles

The default Roles are read-only and cannot be revised or deleted. For example:

- **operator_role**—Includes most Operator permissions.
- **super_admin_role**—Includes all operate and manage permissions (a super-adminuser is any user that has access to all permissions and is assigned to the root-level location).
- **local_admin_role**—Includes a combination of operate and manage permissions.

**Tip**

Select a Role to view the permissions assigned to that Role. See Table 16-3 and Table 16-4 for descriptions of the Operate and Manage roles.

Figure 16-3 Permissions
Selecting a permission may automatically result in the selection of other dependent permissions if the permissions overlap. For example, if you select the Manage Cameras permission, the View Live Video and Perform PTZ permissions are automatically selected. The automatically selected dependent permission(s) cannot be deselected unless the parent permission is deselected first.

Table 16-3 summarizes the Manage permissions:

Click Manage All to select all of the permissions.

Table 16-3 Manage Permissions

<table>
<thead>
<tr>
<th>Manage Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users &amp; Roles</td>
<td>Create, update, or delete user accounts, groups and Roles.</td>
</tr>
<tr>
<td>Cameras</td>
<td>Create, delete, or update Cisco VSM cameras.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only super-admins can perform camera auto-provisioning. See Understanding the Super Admin, page 16-9.</td>
</tr>
<tr>
<td>Servers &amp; Encoders</td>
<td>Create, update, or delete Cisco VSM servers and analog camera encoders.</td>
</tr>
<tr>
<td>Video Walls</td>
<td>Create, update, or delete Video Walls.</td>
</tr>
<tr>
<td>Templates</td>
<td>Create, update, or delete camera templates.</td>
</tr>
<tr>
<td>Schedules</td>
<td>Create, update, or delete schedules.</td>
</tr>
<tr>
<td>Locations &amp; Maps</td>
<td>Create, update, or delete Cisco VSM locations and associated map images.</td>
</tr>
<tr>
<td>Views</td>
<td>Create, update, or delete pre-set video views used to monitor multiple video cameras.</td>
</tr>
<tr>
<td>System Settings</td>
<td>Update Cisco VSM system settings.</td>
</tr>
<tr>
<td>Images</td>
<td>Allows the user to upload firmware images, define the recommended firmware version, and upgrade devices.</td>
</tr>
</tbody>
</table>
Table 16-4 summarizes the *Operate* permissions:

Some permissions are mutually exclusive. For example, you can select either *View Live Video* or *View Secondary Stream Only* but not both at the same time. If you select *View Secondary Stream*, the mutually exclusive permission will be automatically deselected.

Click **Operate All** to select all of the permissions, except *View Secondary Stream Only*.

**Table 16-4 Operate Permissions**

<table>
<thead>
<tr>
<th>Operation Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Live Video</td>
<td>View live video streams from Cisco VSM cameras.</td>
</tr>
<tr>
<td></td>
<td><em>Note</em> If selected, <strong>View Secondary Stream Only</strong> will be automatically deselected.</td>
</tr>
<tr>
<td>View Recordings</td>
<td>View recorded video from Cisco VSM cameras.</td>
</tr>
<tr>
<td>Listen To Audio</td>
<td>Play live or recorded audio from cameras that support audio.</td>
</tr>
<tr>
<td>Export Recordings</td>
<td>Export a video clip to a file.</td>
</tr>
<tr>
<td>Perform PTZ</td>
<td>Use the pan, tilt and zoom controls on cameras that support PTZ.</td>
</tr>
<tr>
<td>Push Video to Wall</td>
<td>Enables the <strong>Publish to Wall</strong> feature in the Cisco Safety and Security Desktop (SASD) application. This feature allows users to change the view shown by all other instances of a selected video wall. The new view is displayed until the dwell time is exceeded.</td>
</tr>
<tr>
<td></td>
<td><em>Note</em> If selected, <strong>View Secondary Stream Only</strong> will be automatically deselected.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Allows all operators to view the alerts for cameras they can access. Users can acknowledge, clear, or comment on an alert (<em>ack/clear/add_user_comment</em>).</td>
</tr>
<tr>
<td>View Analytics Metadata</td>
<td>View the already generated meta data and perform video motion searches (using the Cisco SASD desktop application). Users with only View permissions cannot generate the metadata using Cisco SASD.</td>
</tr>
<tr>
<td>Post Analytics Metadata</td>
<td>Generate the Metadata using Cisco SASD. Users with only Post permission cannot perform searches.</td>
</tr>
<tr>
<td>Control Privacy Mask</td>
<td>Allows operators to enable or disable the Privacy Mask on compatible cameras. All live video from the camera is blocked and cannot be viewed by any operator or monitor, or recorded by the Cisco Video Surveillance system.</td>
</tr>
<tr>
<td>Download Software</td>
<td>Allows users to download the available software installation packages, such as the Review Player EX, Advanced Video Player, and MSI Installation Package.</td>
</tr>
</tbody>
</table>
Understanding the Super Admin

The following operations and functions can only be performed by a super-admin.

A super-admin is any user that has access to all permissions at the root location.

Table 16-5 Super-Admin Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Manager HA</td>
<td>Create, update replace or delete, updating, replacing high availability (HA) configuration for Operations Manager.</td>
</tr>
<tr>
<td>Active Users</td>
<td>Get a list of the active user sessions. The super admin can also log out any active user(s).</td>
</tr>
<tr>
<td>Change user passwords</td>
<td>Change the password for another user.</td>
</tr>
<tr>
<td>Prune History</td>
<td>Prune (delete) old alerts and events.</td>
</tr>
<tr>
<td>Notification policies</td>
<td>Create, update and delete email notification policies.</td>
</tr>
<tr>
<td>Reports</td>
<td>Create, download, and delete reports.</td>
</tr>
<tr>
<td>Custom Event Type Registration</td>
<td>Create, download, and delete custom event types.</td>
</tr>
<tr>
<td>Language Settings</td>
<td>Update the language settings.</td>
</tr>
<tr>
<td>Auto Provisioning Settings</td>
<td>Update the auto provisioning settings for supported camera models.</td>
</tr>
<tr>
<td>LDAP user configuration</td>
<td>Create, download, and delete the LDAP server configuration.</td>
</tr>
</tbody>
</table>
Understanding Dual Login

Dual Login requires that a second user (such as a manager) enter their credentials to approve a user’s access. When the user logs in, a second prompt appears for the manager’s credentials. This optional feature can be used when explicit approval is required whenever a user logs in.

To enable Dual Login, select the **Approval Required** checkbox in a User Group, and then select an “Approval Usergroup”. All users assigned to the User Group can only gain access if a member of the “Approval Usergroup” also enters their password.

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

Provide Access from an LDAP Server (Active Directory)

An LDAP (Lightweight Directory Access Protocol) server can provide Cisco VSM access to members of an external user database. After the LDAP server is added, users from that system can log in to Cisco VSM using the credentials configured on the LDAP server (the users do not need to be added individually to the Operations Manager configuration).

Users select the LDAP domain when logging in to the Operations Manager or Cisco SASD UI.

### Considerations

- Operations Manager uses the LDAP server to authenticate and authorize the user’s username and password.
- LDAP users should be members of user groups in the LDAP configuration since the Operations Manager determines user access privileges based on those LDAP groups. Search filters in the Operations Manager LDAP configuration are used to map the user group(s).
- The number of search filters determine the time it takes for users to log in. A large number or search filters will cause longer wait times for LDAP users logging in. The maximum number of filters is 500.
- Use the Operations Manager Active Users page to view the user groups assigned to LDAP users.
- Users must be in an LDAP organizational unit (OU) that is at least 1 level above the root of the LDAP tree.

### LDAP Best Practices

- LDAP users can be added or removed from the source database without affecting Cisco VSM. When the LDAP user logs in to Cisco Video Surveillance, their credentials are authenticated with the LDAP server, and access is granted or denied based on the LDAP response.
Use LDAP filters to limit the users who can access Cisco VSM.

To delete an LDAP server, you must un-associate the LDAP server from all Cisco VSM user groups.

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

**LDAP Search Filter Settings**

Filters restrict authentication to a subset of users (the filter represents a user group that is defined on the LDAP server). Each filter can be associated with a different user group, which grants LDAP users in that filter the access permissions of the Cisco VSM user group. This allows you to grant different permissions to different sets of users.

For example, a filter for the **dept_eng** users can be associated with an admin user group while rest everyone in **company_eng** will be made an operator.

The maximum number of filters is 500.

<table>
<thead>
<tr>
<th>Table 16-6: LDAP Filter Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>User Search Path</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>User Group Filter</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

See the Cisco Video Surveillance Operations Manager User Guide for additional configuration examples.
Using Locations to Limit User Access

Locations allow you to organize your deployment according to the real-world location of equipment and users. Locations also allow administrators to restrict user access to the specific cameras, policies, and data (such as alerts) required by the user’s role within the organization. For example, while a super-admin has full access to all locations and devices, a local campus administrator might have access only to the devices and policies required to manage a specific site.

Tip
Since all servers, user groups and cameras must be assigned to a location, create the location hierarchy before performing other configuration tasks. Review the information in this section carefully, and then create a location plan to ensure the users in your deployment can access only the equipment, video and policies required for their role.

Refer to the following topics for more information:

- Overview, page 17-2
- Summary Steps, page 17-2
- Understanding Permission-Based and Partition-Based Resources, page 17-3
  - Simple Deployments (User Access to All Devices and Resources), page 17-4
  - Permission-Based Resources: Limiting User Access to Devices, page 17-4
  - Partition-Based Resources: User Access to Templates, Schedules and Other Resources, page 17-5
- Examples: Locations in Simple vs. Large Deployments, page 17-7
Overview

Locations define the physical location of devices, such as cameras, and the logical location of attributes, such as camera templates. This allows system administrators to restrict user access to only the devices and resources required by the different users in a deployment. For example, in a simple deployment, users are assigned to the root level and gain access to all devices and resources. In larger deployments, however, users can belong to user groups that are assigned to locations at lower levels. This restricts the users’ access to the devices at that location (and sub-locations). The users also have access to system resources (such as templates and schedules) that are assigned to other locations.

Summary Steps

To create a location hierarchy, do the following:

Table 17-1  Summary Steps: Location Hierarchy and Assignments

<table>
<thead>
<tr>
<th>Task</th>
<th>More Information</th>
</tr>
</thead>
</table>
| Step 1 Review the overview topics to understand how locations impact users’ ability to access devices and resources. | • Understanding Permission-Based and Partition-Based Resources, page 17-3  
• Examples: Locations in Simple vs. Large Deployments, page 17-7 |
| Step 2 Create the location hierarchy for your deployment. | Cisco Video Surveillance Operations Manager User Guide |
| Step 3 Assign devices, user groups and resources to the locations. | • Cisco Video Surveillance Operations Manager User Guide  
• Controlling User Access Permissions, page 16-1 |
| Step 4 Assign users to one or more user groups. Users gain access to the locations assigned to the user groups. | • Cisco Video Surveillance Operations Manager User Guide  
• Controlling User Access Permissions, page 16-1 |
Understanding Permission-Based and Partition-Based Resources

Locations assigned to Cisco VSM resources define the following:

- The physical location of servers and encoders.
- The installed (physical) and pointed at location of cameras.
- The logical location of Cisco VSM attributes, such as camera templates, schedules, Video Walls and preset Views.
- The location of user groups and user roles.

In addition, the following rules apply:

- Resources such as devices, user groups and view are permission-based, meaning that they can only be accessed by users at that same location or lower (sub-location).
- Partition-based resources (such as templates and schedules) can be accessed by users within the same location hierarchy (locations higher or lower in the same location tree).
- Global resources can be accessed by all users who have the required access permissions.
- Super-admin resources (such as system settings and audit logs) can only be accessed by super-admin users.

Table 17-2 summarizes the resource types.

<table>
<thead>
<tr>
<th>Type</th>
<th>Resources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission-Based</td>
<td>• Devices (cameras, encoders, servers)</td>
<td>Users can access permission-based resources that are assigned to their user group location or lower (sub-location).</td>
</tr>
<tr>
<td></td>
<td>• User groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Views</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, in Figure 17-2 a user assigned to a Dallas Campus user group can access the cameras at the Building 1 sub-location, but not at the Texas location. Dallas users also cannot access any California locations.</td>
</tr>
<tr>
<td>Partition-Based</td>
<td>• User roles</td>
<td>User groups can access partition-based resources that are in the same location hierarchy (either higher or lower, but not in a different branch).</td>
</tr>
<tr>
<td></td>
<td>• Schedules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Camera templates</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, in Figure 17-3 a user assigned to a Dallas Campus user group can access the templates or schedules at any higher or lower level up to the U.S. (root) location. The user cannot, however, access templates or schedules for the Austin Campus or any of the California locations.</td>
</tr>
<tr>
<td>Global Resources</td>
<td>Global resources can be accessed by all users who have the required access permissions.</td>
<td>For example, a user with manage users permissions access all the users in the system. The user object is not restricted to a location.</td>
</tr>
<tr>
<td>Super-admin</td>
<td>• System Settings</td>
<td>Only users assigned to a super-admin user group can access these system-wide resources.</td>
</tr>
<tr>
<td></td>
<td>• Audit Logs</td>
<td></td>
</tr>
</tbody>
</table>
Simple Deployments (User Access to All Devices and Resources)

In a simple deployment (Figure 17-1), all users are assigned to a user group at the root (System) location. Users can access all cameras and resources at all sub-locations.

For example, in Figure 17-1, root (System) level users have access to the devices and resources in all sub-locations, such as California, Texas, and the associated campus and building sub-locations. A user’s ability to view or configure devices and resources is based on the role assigned to their user group.

Figure 17-1  Locations and User Permissions in a Simple Deployment

Tip
User access can still be restricted based on the assigned user group. For example, an operator user group can provide access to only view video, but not configure system resources. See Controlling User Access Permissions, page 16-1 for more information.

Permission-Based Resources: Limiting User Access to Devices

Users can access devices assigned to the same location, or lower. For example, if a user is assigned to a user group at the San Jose Campus location (Figure 17-2), the user gains access to any cameras assigned to the San Jose Campus location, and all sub-locations (such as SJ Building 1).

Note
- Users cannot access cameras assigned to higher locations (such as California in Figure 17-2), or sub-locations in a different hierarchical tree (such as the Milpitas Campus or Texas).
- A user’s location includes all of the user groups to which the user is assigned. For example, if a user is assigned to a user group for the San Jose Campus, and is also assigned to another user group for the Dallas Campus (Figure 17-2), the user gains access to the devices at both locations.
- Devices, user groups and Views are permission-based resources. All permission-based resources adhere to these same rules.
Figure 17-2  Limiting User Access to Specific Locations

- Servers should be assigned to a high-level location to provide support to services, devices and user groups at lower-level locations. In the Figure 17-2 example, assign the servers to either the Root (System) location, or the California and Texas locations.
- Camera Views are also assigned to a location. Users can only access the Views assigned to their location and lower.

**Partition-Based Resources: User Access to Templates, Schedules and Other Resources**

*Partition-based* resources include camera templates, schedules, and user roles. If the user belongs to a user group with access to these resources, then the user can access any partition-based resource in the same location hierarchy (locations that are higher or lower, but not in a different branch).

For example, in Figure 17-3 a user assigned to a *San Jose Campus* user group can access the templates or schedules at any higher level location (up to the U.S. root location). The user cannot, however, access templates or schedules for the *Milpitas Campus* or any of the *Texas* locations.

- The user must be assigned to a user groups that provides access to the resource. See Controlling User Access Permissions, page 16-1 for more information.
Figure 17-3  Limiting User Access to Specific Locations

Understanding Permission-Based and Partition-Based Resources

Resource Location
(Partition-Based Resources)

Device Locations
(Permission-Based Resources)

U.S. (Root)
(super.admin users)

California

Milpitas
Campus

San Jose
Campus

SJ Building 1

SJ Building 2

Texas

Austin
Campus

Dallas
Campus

Dallas Building 1

Floor 1

Floor 2

Resource Location
(Partition-Based Resources)
Examples: Locations in Simple vs. Large Deployments

Simple Deployment Example

A simple Cisco VSM deployment typically places partition-based resources (templates, roles and schedules) at the root level so they can be accessed by users at all of the sub-locations (Figure 17-4). Users must still belong to a user group that provides access to view or manage those resources.

Permission-based resources (such as cameras) can also be placed at the root level, but only users in a user group at the root level will be able to access them. You can assign both devices and users at a sub-location to restrict user access to the permission-based resources at that location.

**Figure 17-4  Example Locations for a Simple Deployment**

<table>
<thead>
<tr>
<th>1</th>
<th>Assign partition-based resources (templates, roles and schedules) to a high-level or root location.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Partition-based resources (templates, roles and schedules) can be viewed and used by all users at all sub-locations.</td>
<td></td>
</tr>
<tr>
<td>• Users can only modify the templates, roles, and schedules that are assigned to their location (or lower).</td>
<td></td>
</tr>
<tr>
<td>• For example, in Figure 17-4 a user assigned to “Milpitas Buildings” can view partition-based resources assigned to the “U.S.” location, but only super-admin users can modify the resources.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> We recommend also assigning servers to a high-level location to provide support to devices and user groups at lower-level locations.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Assign permission-based resources (such as cameras) to sub-locations to restrict user access.</td>
</tr>
<tr>
<td>• Users can only access permission-based resources (such as cameras) that are assigned to the user’s location and lower.</td>
<td></td>
</tr>
<tr>
<td>• For example, in Figure 17-4 a user assigned to “Milpitas Buildings” can access cameras at that level and lower (such as building 1 and building 2), but cannot access cameras at an equal level (such as “San Jose Buildings”) or at higher locations (such as “California” or “US”).</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> Deployments with a small number of users can also assign user groups and permission-based resources to the “U.S.” (root) location.</td>
<td></td>
</tr>
</tbody>
</table>
Large Deployment Example

Larger deployments support multiple campuses or geographically distant sites. Users at different regions or campuses require a distinct set of schedules, roles and templates. For example, the deployment in Figure 17-5 includes sites in both the U.S. and India. *Partition-based resources* (templates, roles and schedules) assigned to the India location can only be viewed by users in the India sub-locations, (not by U.S. users). Resources assigned to the “U.S” location can only be viewed by U.S. users.

This configuration also allows “India” or “U.S.” user to modify the *partition-based resources* for their region without impacting other regions.

*Figure 17-5  Example Locations for a Large Deployment*

<table>
<thead>
<tr>
<th>1</th>
<th>Assign <em>partition-based resources</em> (templates, roles and schedules) to a high-level branch location, such as “U.S.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <em>Partition-based resources</em> (templates, roles and schedules) can be viewed and used by all users within that location hierarchy (for example, from the San Jose Campus up to the System users).</td>
<td></td>
</tr>
<tr>
<td>• Users can only modify the templates, roles, and schedules that are assigned to their location (or lower).</td>
<td></td>
</tr>
<tr>
<td>For example, in Figure 17-5 a user assigned to “California” can view <em>partition-based resources</em> assigned to the “U.S.” location, but not resources in the “India” locations.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Assign <em>permission-based resources</em> (such as cameras) to sub-locations to restrict user access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Users can only access <em>permission-based resources</em> (such as cameras) at their location and lower.</td>
<td></td>
</tr>
<tr>
<td>• For example, in Figure 17-5 a user assigned to “Chennai” can access cameras at that level and lower (such as “CH Bldg 1”), but cannot access cameras at an equal level (such as “Bangalore”) or at higher level (such as “India”).</td>
<td></td>
</tr>
</tbody>
</table>

---

**Tip**

System users (such as super-admins) can view all resources at all sub-locations. Super-admins can also access system settings and other resources. See Table 17-2 on page 17-3 for more information.
PART 8

Video Events and Analysis
Using Events to Trigger Actions

Events and alerts reflect changes to system and device health, or security events that occur in the system. These events and alerts can be viewed in a monitoring application (such as Cisco SASD), generate notifications, or trigger additional actions.

Refer to the following topics for more information:

- Understanding Events and Alerts, page 18-2
  - Health and Security Event Types, page 18-3
  - Triggering Actions Based on Alerts and Events, page 18-3
Understanding Events and Alerts

Events represent incidents that occur in the system and devices. Alerts aggregate (group) those events together for notification purposes. For example, if a camera goes offline and comes back online repeatedly, the individual events for that issue are grouped under a single alert, which results in a single notification. This prevents operators from being flooded with notifications for every event that occurs for the same issue.

**Note**

The alert severity reflects the severity of the most recently generated event. For example, if a camera becomes unreachable and the streaming status is Critical, the alert is Critical. When the camera becomes reachable again, and the streaming status normal event occurs, and the alert severity is changed to INFO.

Figure 18-1 summarizes how Cisco VSM events and alerts are generated, viewed and managed.

**Figure 18-1  Health Events, Alerts, and Notifications**

1. Events are generated by cameras, encoders and Media Servers.
2. The Cisco VSM Operations Manager aggregates the events into alerts:
3. The browser-based Operations Manager can be used to view events, send notifications, or (optionally) perform actions that are triggered by security events (such as motion detection).

4. Additional monitoring applications can also be used to view events and alerts:
   - The Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application can be used to view alerts, related events, and related video. You can also change the alert state, add comments, close the alert, and perform other management options.
   - Custom applications can be written to gather information, change the alert status, add comments, or trigger actions when an event or alert occurs. See the Cisco Video Surveillance API Programming Guide for more information.

---

**Note**

Custom applications can also subscribe to ActiveMQ topics to receive notifications about device and system changes. For example, the Alerts topic notifies subscribers when any alert occurs in the system. The custom application can use the ActiveMQ message contents to optionally trigger additional notification or actions. See the Cisco Video Surveillance API Programming Guide for more information.

---

### Health and Security Event Types

Cisco VSM generates two types of events: device health events and security events:

- **Health Events** are generated when a device health change occurs, such as reachability, fan speed, file system usage, or other device-related issues. Critical health events generate alerts by default.
- **Security Events**—Events such as motion start or stop, analytics, contact closures, or soft triggers from an external system can be configured to generate alerts, or perform other actions. Security events do not generate alerts by default.

### Triggering Actions Based on Alerts and Events

The Operations Manager includes the following built-in features to trigger notifications and other actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical health notifications</td>
<td>Use the Health Notifications feature to send notifications when a critical device error occurs. Critical errors are health events that impact the device operation or render a component unusable. For example, a Media Server that cannot be contacted on the network, or a camera that does not stream or record video.</td>
<td>“Sending Alert Emails (Notification Policies)” in the Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
</tbody>
</table>
### Understanding Events and Alerts

Motion event notifications: Click **Alert Notifications** in the camera template to enable or disable the alerts that are generated when a motion event stops or starts.

**Templates section of the Cisco Video Surveillance Operations Manager User Guide**

Trigger actions when a security event occurs: Use the Advanced Events feature (in the camera template) to trigger a variety of actions when a security event occurs.

For example, you can send alerts only on motion start, on motion stop, stop or start video recording, record video for a specified length of time, invoke a URL, move a camera position to a specified PTZ preset, or display video on a Video Wall.

**Advanced Events section of the Cisco Video Surveillance Operations Manager User Guide**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion event notifications</td>
<td>Click <strong>Alert Notifications</strong> in the camera template to enable or disable the alerts that are generated when a motion event stops or starts.</td>
<td>Templates section of the Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
<tr>
<td>Trigger actions when a security event occurs</td>
<td>Use the Advanced Events feature (in the camera template) to trigger a variety of actions when a security event occurs. For example, you can send alerts only on motion start, on motion stop, stop or start video recording, record video for a specified length of time, invoke a URL, move a camera position to a specified PTZ preset, or display video on a Video Wall.</td>
<td>Advanced Events section of the Cisco Video Surveillance Operations Manager User Guide</td>
</tr>
</tbody>
</table>
Using Video Analytics for Post-Event Motion Detection

Video analytics are used to analyze images for attributes and events that occur within the image. For example, Luminance metadata that is generated for a video feed can be used to perform Video Motion Search using the Cisco Video Surveillance Safety and Security Desktop (Cisco SASD) application (or a third party monitoring application).

To enable a metadata track, a Metadata Server must be added to the Operations Manager, and the metadata track must be enabled on a camera template. Cameras added to that template will generate a lower-resolution version of the recorded video that includes the metadata information. That metadata track is then accessed by Cisco SASD or a third party application to analyze the video.

Configuring and Using Video Analytics

To configure video analytics, see the Cisco Video Surveillance Operations Manager User Guide.

To analyze metadata tracks (such Video Motion Search), the Cisco SASD desktop application must be installed on a monitoring PC. See the Cisco Video Surveillance Safety and Security Desktop User Guide for more information.

Network Design Considerations

Metadata generation requires a high level of network communication between the Cisco Metadata server and Cisco Media Server where the recordings are stored and supported. Because of this, the servers should be placed in the same network. If the Cisco Media Server is located in a remote or low-bandwidth location, problems can occur which interfere with metadata generation.
Part 9

Integrating External Systems
Using ActiveMQ to Monitor Cisco VSM

ActiveMQ is message-oriented middleware (MOM) that allows client applications to subscribe to a variety of topics to receive event notifications about changes to the Cisco VSM configuration or status. This allows changes on a device to be reflected on all clients.

For example, if a user deletes a device, or the device health or status changes, the changes will be updated on all clients.

In Figure 20-1, a custom application subscribes to ActiveMQ messages are sent to a custom application which transmits the message payload to a monitoring app.

See the Cisco Video Surveillance API Programming Guide for more information.
Using the Cisco VSM APIs and SDK

The Cisco Video Surveillance (Cisco VSM) APIs are used to display video from a Cisco VSM in a custom client application. There are two main categories of APIs:

- Operations Manager APIs—Used to gather information about the system, including cameras, Media Servers, system and device health, security events and alerts, and other data.
- The workstation monitoring APIs—Used to display video in a custom application using one of the methods described in Figure 21-1.

Figure 21-1 summarizes the types of client applications used to display Cisco VSM video, and the APIs, commands and methods used by each application type.
See the *Cisco Video Surveillance API Programming Guide* for more information. This document also describes additional features, such as ActiveMQ messaging, Cisco VSM events and alerts, commands and methods that can be sent directly to a Media Server, and the security sessions used when interacting with either a Operations Manager or a Media Server.

**Understanding the Cisco VSM Software Development Kit (SDK)**

The Cisco VSM SDK provides tools and examples to help application developers create custom user interface applications. The SDK examples are written in C# using Microsoft Visual Studio 2012. The SDK also includes a number of helper classes for basic functions, such as logging in, managing a sessionID, and managing cameras. The **CameraSupport** directory provides sample commands for displaying multi-pane, single-pane and RTSP video. Examples are provided to gather system health, available recordings, thumbnails, alerts, and soft triggers. You can also verify if a camera supports PTZ movements.

**Note**

The VSM SDK is available on the Physical Security community in the Cisco Developer Network (CDN). CDN membership is extended to qualified Cisco Ecosystem Technology Partners. Contact your account team for more information.
Related Documentation

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

- Click **Help** at the top of the screen to open the online help system.
- 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>
<thead>
<tr>
<th>Table B-1 Revision History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document Revision Date</strong></td>
</tr>
<tr>
<td>August, 2015</td>
</tr>
</tbody>
</table>