CHAPTER 10

Using the VSM Management Console

The VSM Management Console provides a web-based interface through which you can perform various system configuration and management operations and see important information for Cisco Video Surveillance Media Server (VSMS), Cisco Video Surveillance Operations Manager (VSOM), and Cisco Video Surveillance Virtual Matrix (VSVM). The pages and options that are available from the Management Console depend on the type of system (VSMS, VSOM, or VSVM) that you are using it for and on installed VSM components.

This chapter includes these topics:

Accessing and Exiting the Management Console

To access the Management Console, use any method that Table 10-1 describes. Each method starts a Management Console for the corresponding VSM application. When you access the Management Console, it appears in a new browser window.

The default user name for logging in to the Management console is **root** and the default password is **secur4u**. For information about changing the password, see the "Management Console Password Page" section on page 10-24.

Table 10-1 Methods for Accessing the Management Console

Method	Remarks	Procedure
Accessing the Management Console for a VSOM or VSMS host by using its IP address or host name.	This procedure does not work if you have chosen the **Change default homepage to VSOM** option. (See the Operations Manager Configuration Page, page 10-19 for more information.)	From a PC that is on the same network as the host, enter the IP address or host name of the VSOM or VSMS host in a supported web browser.
Accessing the Management Console from the VSOM web interface.	This method provides access only to VSMS hosts that have been configured in VSOM.	1. Access VSOM as described in the "Accessing VSOM" section on page 1-4. 2. In the VSOM Operator page, click the **Admin** link, which appears near the top left of the page. 3. Click the **Servers** link under Devices to display a list of configured servers. 4. In the Console column, click the Cisco logo that appears in the row of the system for which you want to display the Management Console. 5. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.
Accessing the Management Console from the keyboard and monitor that are attached to a VSMS system.	You can use this method to access the Management Console for VSMS systems that are not yet configured in VSOM.	1. Click the Management icon on the server desktop:  2. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.
Accessing the Management Console from your PC.	You can access the Management Console for a VSMS from a PC that is on the same network as the VSMS system.	1. Start a web browser and enter the following address, where <*server*> is the IP address or host name of the VSOM host: **http://<*server*>/vsmc.html** 2. If a pop-up window prompts you to log in, enter your VSMS user name and password and click **OK**.

To exit the VSM Management Console, exit the browser window in which it appears.

Overview Pages

The Management Console provides the following overview pages:

- Installed Packages—Displays a list of installed and driver packages. For more information, see the "Installed Packages Page" section on page 10-3.
- Status Console—Provides current and historical information about system performance and resource use. For more information, see the "Status Console Page" section on page 10-3.
- Raid Status—Provides information about the Redundant Array of Independent Disks (RAID) on a system, if applicable. For more information, see the "RAID Status Page" section on page 10-5.

Installed Packages Page

The Installed Packages page appears when you access the Management Console from the VSOM Administration Area. You also can display the Installed Packages page by clicking the **Installed Packages** link under Overview at the left side of the Management Console.

The Installed Packages page displays this information:

- Installed Packages—Lists the VSM packages that you have installed.
- Additional Driver Packages—Lists the VSM drivers that you have installed for cameras and encoders. For related information, see the "Manage Drivers Page" section on page 10-15.

Status Console Page

The Status Console Overview page displays a set of graphical reports that show various information about performance and resource use of a VSMS system. This page also provide access to reports that provide historical performance and resource use data. You can use the information that the Status Console page provides to monitor and review system performance.

To display the Status Console page, click the **Status Console** link under Overview at the left side of the Management Console.

Viewing Current Reports

When the Status Console Overview page appears, it displays the following reports for the VSMS system. These reports show information that is current at the time that you display the page. To update reports, refresh your browser, or exit and then access the Status Console page.

- CPU (user and system) Load %—Displays the CPU resources that are consumed by users and by system operations, as a percentage of total CPU capacity.
- CPU Load Avg—Displays the average CPU resources that are consumed by users and the average CPU resources that are consumed by system operations, as a percentage of total CPU capacity. The system calculates averages at 5-minute intervals.
- Disk Usage—Displays the amount of disk space used on the root and /usr disks for system files, archives, and related files, as a percentage of total capacity of these disks.
- Free Memory—Displays the amount of RAM used and the amount of free RAM.
- New TCP Connections—Displays the number of existing TCP connections to and from the server.

- Traffic Analysis—Displays the amount of incoming and outgoing network traffic, in bytes per second.

Viewing Historical Reports

To display historical versions of any Status Console report, click the report name or graph in the Status Console Overview page. Historical reports include the following:

- Daily graph—Provides information for the past 32 hours, calculated by averaging values every 5 minutes. The information in this graph is the same as the information that appears in a graph on the Status Console Overview page.
- Weekly graph—Provides information for the past 8 days, calculated by averaging values every 30 minutes.
- Monthly graph—Provides information for the past 4 weeks, calculated by averaging values every 2 hours.
- Weekly graph—Provides information for the past 12 months, calculated by averaging values every 1 day.

Some reports also include a table of maximum, average, and current values.

To return to the Status Console Overview page from any page that displays historical reports, click the **Return to Status Console** index link at the top or bottom of the page.

Understanding Reports

Status Console reports provide information as follows:

- The time scale at the bottom of a graph progresses from left to right, as indicated by a small red arrow at the right of the scale. The time that the report generates appears at the far right of the time scale.
- The vertical red line indicates a start of a new period as follows:
  - Daily report—12:00 a.m. (00:00)
  - Weekly report—12:00 a.m. (00:00) on Monday
  - Monthly report—First day of the month
  - Yearly report—First day of the year (January 1)

The green shaded area provides information as follows:

  - CPU (user and system) Load % report—Displays the CPU resources that are consumed by users and by system operations, as a percentage of total CPU capacity.
  - CPU Load Avg report—Displays traffic load on the server, as a percentage of total CPU capacity.
  - Disk Usage report—Displays the amount of disk space use on the /usr disk of the server, as a percentage of total disk capacity.
  - Free Memory graph—Displays the amount of free memory on the server, in bytes
  - New TCP Connections graph—Displays the number of new incoming TCP connections.
  - Traffic Analysis graph—Displays the amount of incoming network traffic, in bytes per second.

- The blue line provides information as follows:
  - CPU (user and system) Load % report—Displays the server CPU use, as a percentage of total CPU capacity.
  - CPU Load Avg report—Displays traffic load on the server, as a percentage of total CPU capacity.
  - Disk Usage report—Displays the amount of space that is used for incoming traffic on the /usr disk of the server, as a percentage of total disk capacity.
  - Free Memory report—Displays the total amount of total memory, in bytes
  - New TCP Connections report—Displays the number of new outgoing TCP connections.
  - Traffic Analysis report—Displays the amount of outgoing network traffic, in bytes per second.
- The dark green line displays the maximum value for incoming traffic, calculated every 5 minutes. This line does not apply to the Traffic Analysis reports.
- The magenta line displays the minimum value for incoming traffic, calculated every 5 minutes. This line does not apply to the Traffic Analysis reports.

RAID Status Page

The RAID Status page displays information about the RAID, if it is installed on a Cisco Multiservice Platform that includes an LSI MegaCLI compliant RAID controller. This page also lets you silence alarms that occur when a RAID failure occurs or when the RAID array is rebuilding, and generate a debug package.

To display the RAID Status page, click the **Raid Status** link under Overview at the left side of the Management Console.

The Raid Status page includes these areas:

- VSM RAID Viewer area—The left side of this area provides general information about the RAID that is installed on the system and shows the version of the BIOS that the system is running.

  The center of this area includes these button:
  - **Refresh Status**—Click to update the information on the page with the most current data.
  - **Silence Alarms**—Click to silence the alarm that sounds when a RAID failure occurs or when the RAID array is rebuilding.
  - **Create Debug Package**—Click to create zip file that contains RAID controller log files, then follow the prompts that appear to download the zip file to your PC. The Cisco Technical Assistance Center (TAC) may request the debug package if you need assistance with troubleshooting a RAID issue.

  The right side of this area provides links that you can click to quickly display other areas of the RAID Status page.
- Disk Usage area—Provides information about the RAID file systems.
- Virtual Disks Summary—Provides summary information about the virtual disks in the RAID.
- Physical Disks Summary—Provides summary information about the physical disks in the RAID.
- Virtual Disks Details—Provides detailed information about the virtual disks in the RAID.
- Physical Disks—Provides detailed information about the physical disks in the RAID.
- Disk Error Definitions—Defines various RAID error types that can occur.

Monitoring Pages

The Management Console provides the following monitoring pages:

- Archives—Displays and provides access to information about archives. For more information, see the "Archives Page" section on page 10-6.
- Archive Backup—Displays and provides access to information about archives that are backed up on the system. For more information, see the "Archive Backup Page" section on page 10-9.
- System Log—Lets you display information from the system log files. For more information, see the "System Log Page" section on page 10-10.
- Mediaout—Displays and provides access to information about current Mediaout, HTTP, and RTSP connections to the server. For more information, see the "Mediaout Page" section on page 10-11.
- Server Status—Displays information about processes and components on this system. For more information, see the "Server Status Page" section on page 10-12.

Archives Page

The Archives page displays and provides access to information about archives that are configured for your VMS system.

To display the Archives Overview page, click the **Archives** link under Monitoring at the left side of the Management Console. The Archives Overview displays this information:

- Total number of Archives—Number of archives that are configured
- Current Recording Rate—Rate, in Mbps, at which data is being written to the server. You can use this information to calculate when the server will reach its storage capacity and to determine appropriate retention periods.

Viewing Information About Archives

You can view information about archives from the Archives Overview page as follows:

- To Display a list of all archives, click the **View All Archives** link. A list of all archives appears. Table 10-2 describes the information that the list provides.

Table 10-2 Archive Information

Item	Description
Archive Name	Name that you configured when you set up the archive. To see detailed information about the archive, click its name. The "Understanding Archive Details" section on page 10-8 describes the information that appears.
Archive Type	Type that you configured when you set up the archive: • Regular—The archive is configured as a regular archive, which runs for a set duration • Loop—The archive is configured as a loop archive, which repeats contains data for a set duration • Clip—A portion of an archive • BWM—Proprietary clip that can be played by using the Cisco ReView Player • BWX—Password-protected proprietary clip that can be played by using the Cisco ReView Player • Backup—Archive that is backed up to another VSMS
Archive Status	Whether the archive is recording: • SHELVED—Archive has stopped recording. (A regular or loop archive can be started again.) • RUNNING—Archive is actively recording
Archive Media	Type of data in the archive (for example, MPEG-4 or JPEG).
Archive Expiry	When the archive is configured to expire. Data in an archive is removed after this time. A value of 0 indicates that the archive does not expire.
Archive Size	Amount of disk space that the archive is currently using.
Storage Est.	Amount of disk space that has been reserved for the archive. If there is not sufficient space, an archive does not start.
Archive Duration	For a regular archive, indicates how long the archive runs. For a loop archive, indicates the length of time in the loop.
Retention	Percentage of the archive that is currently stored on the server. This value is calculated as follows (Table 10-3 explains each of the variables in this calculation): (Archive Stop Time – Archive Start Time) / Archive Duration A value of 1 or greater appears as 100%.

- To see detailed information about all archives, click the **View complete details of all Archives** link. The "Understanding Archive Details" section on page 10-8 describes the information that appears.
- To see detailed information about a specific archive, choose the archive from the drop-down list at the bottom of the page, then click the **View** button. The "Understanding Archive Details" section on page 10-8 describes the information that appears.

Understanding Archive Details

When you display detailed information about an archive by clicking its name, as described in the "Viewing Information About Archives" section on page 10-6, you see the information that Table 10-3 describes.

Table 10-3 Archive Details

Item	Description
Archive Name	Name that you configured when you set up the archive.
Archive Status	Whether the archive is recording: • SHELVED—Archive has stopped recording. (A regular or loop archive can be started again.) • RUNNING—Archive is actively recording
Storage Path	Location of archive on the server.
Archive Type	Type that you configured when you set up the archive: • Regular—The archive is configured as a regular archive, which runs for a set duration • Loop—The archive is configured as a loop archive, which repeats contains data for a set duration • Clip—A portion of an archive • BWM—Proprietary clip that can be played by using the Cisco ReView Player • BWX—Password-protected proprietary clip that can be played by using the Cisco ReView Player • Backup—Archive that is backed up to another VSMS
Archive Duration	For a regular archive, indicates how long the archive runs. For a loop archive, indicates the length of time in the loop.
Archive Media	Type of data in the archive (for example, MPEG-4 or JPEG)
Video Width	Width in pixels of the video image in the archive.
Video Height	Height in pixels of the video image in the archive.
Video Quality	Recording quality of stream, on a scale from 1 to 100. A higher number represents higher quality but consumes more disk space.
Video Framerate	Framerate of the video. Applies to JPEG streams only.
Video Bitrate	Bitrate of the video. Applies to non-JPEG streams only.
Archive Expiry	When the archive is configured to expire. Data in an archive is removed after this time. A value of 0 indicates that the archive does not expire.
Archive Size	Amount of disk space that the archive is currently using.
Archive Storage Est	Amount of disk space that has been reserved for the archive. If there is not sufficient space, an archive does not start.

Table 10-3 Archive Details (continued)

Item	Description
Archive Start Time	• For regular archives, date and time of first frame found on the disk. • For loop archives, date and time of first frame found on the disk. • For clips, start date and time of the clip. 0 indicates that no data was found for this clip. • For BWM or BWX clips, start date and time of the clip. • For backup archives, date and time of first frame found on the disk • For a backup clips (a backup of a non BWM or BWX clip, start time of the clip. 0 indicates that no data was found for this clip.
Archive End Time	• For regular archives, date and time of last frame found on the disk. • For loop archives, date and time of last frame found on the disk. • For clips, end date and time of the clip. 0 indicates that no data was found for this clip. • For BWM or BWX clips, end date and time of the clip. • For backup archives, date and time of last frame found on the disk • For a backup clips (a backup of a non BWM or BWX clip, end time of the clip. 0 indicates that no data was found for this clip.
Archive Create Time	For BWM and BWX clips, date and time that the clip was created.
Event Archive	Indicates whether the archive was created due to an event occurring (yes or no).
Recording Rate	Recording rate of the archive, in Mbps.
Max Fps	Maximum number of frames per second in the archive.
Max Frame Size	Maximum frame size in the archive.
Current Duration	Current length of the archive, calculated as: Archive End Time – Archive Start Time
Current Retention	Percentage of the archive that is currently stored on the server. This value is calculated as follows: (Archive Stop Time – Archive Start Time) / Archive Duration A value of 1 or greater appears as 100%.

Archive Backup Page

The Archive Backup page displays information about archives that are backed up on this server.

To display the Archive Backup page, click the **Archive Backup** link under Monitoring at the left side of the Management Console. The Archive Backup page displays the summary information that Table 10-4 describes.

Table 10-4 Archive Backup Summary Information

Item	Description
Archive Name	Name that you configured for the archive
Backup Status	Displays Succeeded for a backup that completed or Failed for an archive that did not complete
Start Time	Date and time that the backup started
End Time	Date and time that the backup completed
Number of files sent	Number of archive files sent to this backup server

To see detailed information about an archive backup, click its name in the list. The system displays a report that includes the information that Table 10-5 describes.

Table 10-5 Archive Backup Detailed Information

Item	Description
Archive name	Name that you configured for the archive
Archive status	Displays Succeeded for a backup that completed or Failed for an archive that did not complete
Start Time	Date and time that the backup started
End Time	Date and time that the backup completed
No. of files sent	Number of archive files sent to this backup server
No. of bytes sent	Number bytes in all files sent to this backup server
Last file send time	Date and time that the last file in the backup was sent to this backup server
Log file size	Size in bytes of the archive backup log file
Log file	Displays the contents of the log file, which includes additional information about the archive backup

System Log Page

The System Log page lets you display up to 400 lines from the VSMS log files.

To display the System Log page, click the **System Log** link under Monitoring at the left side of the Management Console.

To display information from a system log, follow these steps:

Procedure

Step 1 Click the **System Log** link under Monitoring at the left side of the Management Console.

The System Log page appears.

Step 2 From the **Select log file to view** drop-down list, choose the log file for which you want information:

Choices are:

- **ims.log**—Primary VSMS log file. Includes system error messages and system activity messages.
- **httpd.access**—Includes HTTP requests that the VSOM or VSMS host sends to the Apache server.
- **httpd.errors**—Apache server error log.
- **snmpd.log**—Includes information about the snmp daemon, such as when the snmp daemon starts, stops, the snmpd.conf configuration file is read by the daemon.

Step 3 From the **Select number of recent lines to view** drop-down list, choose the number of log file entries that you want to view.

The system can display the most recent 100, 200, 300, or 400 entries.

Step 4 Click the **View** button.

Mediaout Page

The Mediaout page displays and provides access to information about video that the VSMS system is serving. VSMS uses a Mediaout connection to serve video.

To display the Mediaout Overview page, click the **Mediaout** link under Monitoring at the left side of the Management Console. The Mediaout Overview page displays this information:

- Total number of Mediaout Connections—Number of HTTP and RTSP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an HTTP or RTSP connection.
- Bandwidth of all Mediaout Connections—Total bandwidth that is consumed by all Mediaout connections.
- Total number of HTTP Connections—Total number of HTTP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an HTTP connection.
- Bandwidth of HTTP Mediaout Connections—Total bandwidth that is consumed by all HTTP Mediaout connections.
- Total number of RTSP Connections—Total number of RTSP connections that live or archived video is being served to. Indicates the number of users who are viewing video through an RTSP connection.
- Bandwidth of RTSP Mediaout Connections—Total bandwidth that is consumed by all HTTP Mediaout connections.

Viewing Information About Mediaout Connections

You can view detailed information about Mediaout connections from the Mediaout Overview page by clicking the following links:

- **View details of all Mediaout connections**—Provides detailed information about all HTTP and RTSP connections that are serving live or archived media feeds
- **View details of all HTTP connections**—Provides detailed information about HTTP connections that are serving live or archived media feeds

- **View details of all RTSP connections**—Provides detailed information about RTSP connections that are serving live or archived media feeds
- **View details of all live media connections**—Provides detailed information about HTTP or RTSP connections that are serving live media feeds
- **View details of all recorded media connections**—Provides detailed information about HTTP or RTSP connections that are serving archived media feeds

To view detailed information about a specific proxy or archive connection, choose the name of the connection from the drop-down list at the bottom of the page, then click the **View** button. A proxy connection is used for live video and an archive connection is used for recorded video.

For a description of the detailed information that you can view, see the "Understanding Media Out Connection Details" section on page 10-12.

Understanding Media Out Connection Details

When you display detailed information about a Mediaout connection as described in the "Viewing Information About Mediaout Connections" section on page 10-11, you see the information that Table 10-6 describes.

Table 10-6 Mediaout Connection Details

Item	Description
Protocol	Protocol that the Mediaout connection uses (HTTP or RTSP)
Type	Type of stream that is being viewed (live or recorded)
Name	Name of the live or recorded stream that is being viewed
Media	Type of media in the stream (for example, MPEG or JPEG)
IP Address	IP address of the client PC that is viewing the stream
Port	Port on the server from which the stream is being sent
Uptime	How long the stream has been being running
Transport Type	Transport protocol used for the stream (TCP or UDP)
Avg Bandwidth	Average bandwidth used by the stream, in bytes per second
Avg FPS	Average frames per second send in the stream
Lost Frames	Number of frames dropped by the stream
RTP loss	Number of RTP packets dropped by the stream

Server Status Page

The Server Status page displays status information about VSMS processes and components.

To display the Server Status page, click the **Server Status** link under Monitoring at the left side of the Management Console.

Configuration Pages

The Management Console provides the following configuration pages:

- SNMP Trap Destinations—Displays information about the SNMP service status and lets you configure SNMP trap destinations. For more information, see the "SNMP Trap Destinations Page" section on page 10-13.
- Manage Drivers—Lists driver packages that are installed on the Media Server and lets you upload, install, and uninstall driver packages. For more information, see the "Manage Drivers Page" section on page 10-15.
- Media Server—Provides information about Media Server settings and provides options for configuring several basic parameters. For more information, see the "Media Server Configuration Page" section on page 10-17.
- Media Server Backup—Lets you create and store a backup file that contains Media Server configuration information. For more information, see the "Media Server Backup Page" section on page 10-19
- Operations Manager—Provides information about VSOM settings and provides options for configuring several basic parameters. For more information, see the "Operations Manager Configuration Page" section on page 10-19.
- Operations Manager Backup—Lets you create and store a backup file that contains VSOM configuration information. For more information, see the "Operations Manager Backup Page" section on page 10-23.
- Virtual Matrix—Lets you designate the port number on which Video Surveillance Virtual Matrix clients communicate with the VSMS host. For more information, see the "Virtual Matrix Configuration Page" section on page 10-24.
- Console Password—Lets you designate the password that must be entered to access the Management Console. For more information, see the "Management Console Password Page" section on page 10-24.
- Camera Firmware Upgrade—Lets you upgrade the firmware on one or more cameras in your video surveillance deployment. For more information, see the "Camera Firmware Upgrade Page" section on page 10-25
- Server Upgrade—Lets you upgrade the VSMS software that is running on the VSMS host. For more information, see the "Server Upgrade Page" section on page 10-27.
- Restart Server—Lets you restart VSM applications on the server that you are accessing. For more information, see the "Restart Server Page" section on page 10-28.
- Reboot Server—Lets you reboot (power cycle) the server that you are accessing. For more information, see the "Reboot Server Page" section on page 10-29.
- Shutdown Server—Performs a graceful shutdown of the server. For more information, see the "Shutdown Server Page" section on page 10-29.

SNMP Trap Destinations Page

The SNMP Trap Destinations page displays information about the SNMP service status. It also lets you configure SNMP trap destinations.

To display the SNMP Trap Destinations page, click the **SNMP Trap Destinations** link under Configuration at the left side of the Management Console.

Viewing SNMP Trap Status

The top part of the SNMP Trap Destinations page displays the SNMP service status, which can be either of the following:

- On—SNMP service is operating. This state is the system default.
- Off—SNMP service has not started, has been stopped, or has failed. To troubleshoot this issue, start by issuing the following Linux command on the VSMS host to check the status of the SNMP service: **/etc/init.d/cisco status**.

Downloading the VS Event MIB

SNMP trap receivers on client SNMP servers use a management information block (MIB) to interpret traps that they receive from a VSMS host.

To view the MIB file, click the **VS Event MIB** link.

Configuring SNMP Trap Destinations

The system automatically configures the VSOM host as a trap destination. You can configure up to five SNMP additional trap destinations. To do so, perform the following steps.

Note
- VSM supports SNMP version 2 (Inform)
- Running a third-party trap receiver on a VSM host is not supported

Procedure

Step 1 Click the **SNMP Trap Destinations** link under Monitoring at the left side of the Management Console.

The SNMP Trap Destinations page appears.

Step 2 In the IP Address/Host Name field for the trap that you are configuring, enter the IP address or host name of the server to receive SNMP traps.

Leading protocol strings (for example, http://) and port numbers (for example, 8080) are not allowed.

Repeat this step for each trap that you want to configure.

Note The first option in this field indicates the VSOM host that the system has automatically configured as an SNMP trap destination. This first option is not configurable.

Step 3 Click the **Update** button.

To remove a trap destination, delete the information in the IP Address/Host Name field, then click **Update**.

Manage Drivers Page

The Manage Drivers page lists driver packages that are installed on the Media Server. It also lets you upload, install, and uninstall driver packages. Driver packages enable the use of various Cisco and third-party cameras and encoders with VSM.

To display the Manage Drivers page, click the **Manage Drivers** link under Configuration at the left side of the Management Console.

Viewing a List of Driver Packages

The Driver packages area of the Manager Drivers page lists the driver packages that are on the Media Server. The list includes the version number of each driver package. The designation [“installed]” indicates that VSMS can be used with the device that the driver supports.

Uninstalling a Driver Package

Uninstalling a driver package makes is unavailable for use. This process does not remove the driver package from the system. You can reinstall it at any time.

To uninstall a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 From drop-down list in the Uninstall Driver Package area, choose the driver package that you want to uninstall.

This list includes all driver packages that are installed on this server.

Step 3 Click the **Uninstall** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so to ensure that the uninstall process completes.

Installing a Driver Package

When you install a driver package, the system automatically uninstalls other version of the driver package that are installed on the Media Server. An uninstalled driver package is not removed from the VSMS host.

Use this process to install a driver package that you have uninstalled and that is stored on the VSMS host. To install a driver package that is not stored on the VSMS host, see the “Uploading a Driver Package” section on page 10-16.

To install a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 From drop-down list in the Install Driver Package area, choose the driver package that you want to install.

This list includes all drivers that are stored on the VSMS host.

Step 3 Click the **Install** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so before using the devices that are associated with the driver package to ensure that the devices function properly with VSM.

Uploading a Driver Package

Uploading a driver package copies a driver package that you downloaded from Cisco.com to the VSMS host and then installs the driver package. You can use this procedure when you need to update the Media Server with a new driver package or you need to install a driver package for a new device.

Before you begin, download the driver package to a PC that you can access from the system on which you are running the Management Console.

To download a driver package go to http://www.cisco.com/go/physicalsecurity, click the **Products** link, then click the **Cisco Network-Centric Video Surveillance products** link. See the Download Software section on the page for information about obtaining driver packages. You must have a valid support contract or registration to access this web site.

To upload and install a driver package, follow these steps:

Procedure

Step 1 Click the **Manage Drivers** link under Monitoring at the left side of the Management Console.

The Manage Drivers page appears.

Step 2 In the field for the driver name in the Install Driver Package area, enter the full path and file name of the driver package to upload.

You can use the **Browse** button to locate the driver package.

Step 3 Click the **Upload** button.

The Management Console indicates the operations that it performs and give you the option to restart VSMS.

The system validates the driver package and displays an error message if it is not valid.

Step 4 Take either of these actions:

- To restart VSMS, click where indicated, then click the **Restart Now** button.
- To return to the Manage Drivers page without restarting VSMS, click where indicated.

If you do not restart VSMS now, make sure to do so before using the devices that are associated with the driver package to ensure that the devices function properly with VSM.

Media Server Configuration Page

The Media Server Configuration page provides information about Media Server settings and provides options for configuring several basic parameters. This page also provide options for configuring archive storage repositories.

To display the Media Server Configuration page, click the **Media Server** link under Configuration at the left side of the Management Console.

If you change any options in the Media Server Configuration page, you must click the **Update** button at the bottom of the page to save the changes. To discard the changes, exit the page by choosing another page or exiting the browser.

If addition, after changing any options in the Media Server Configuration page you must restart the VSMS host as described in the "Restart Server Page" section on page 10-28.

To update options to their last-saved values, click the **Reset** button, then click the **Update** button to save the changes.

Cisco recommends that you back up the VSMS configuration whenever you make changes to it. For instructions, see the "Media Server Backup Page" section on page 10-19.

Table 10-7 describes the options in the Media Server Configuration page.

Table 10-7 Media Server Configuration Page Options

Option	Description
Storage Configuration	
Max Storage %	Specifies the maximum amount of space that recorded data can consume on a storage volume as a percentage of the total disk space on the volume. This configuration applies to all volumes. Valid values are numbers 1 through 98. The default value is 98.
PTZ Configuration	
Camera Control Lockout	Designates how a camera behaves if PTZ contention occurs. (Contention occurs when two resources simultaneously attempt to access a camera PTZ operations.) In this case, the camera responds to PTZ commands from the first resource. It accepts PTZ commands from the next resource when the first resource is idle for the amount of time that this option defines. The default value is 5 minutes.
Media Out Ports	
HTTP Port	*Display only.* The port on the VSMS host to be used for HTTP out connections.

Table 10-7 Media Server Configuration Page Options (continued)

Option	Description
RTSP Port	The port on the VSMS host to be used for RTSP out connections. Valid values are integers 1 through 65535. The default value is 554. Unless there is a network requirement it is recommended that the default port be used because it is the standard RTSP port.
Proxy Port	The port on the VSMS host to be used for video proxy out (live media) connections. Valid values are integers 1 through 65535. The default value is 9090. Unless it is being used by another system process, it is recommended that the default port be used.
RTP Port Range	The port on the VSMS host to be used for RTP out connections. Valid values are integers 1024 through 49151. Separate a range of values with a dash (-). For example, 2024-2052.
Local Repositories	
Local Archive Repositories	Displays a list of available partition mounts on the server where recordings can be stored. VSMS can recognize up to 500 partitions mounts. Repositories in red are unmounted locations. This 500 partition mount limit includes the partitions specified in the Local Repository, Clipping (BWM and BWX), and Back-up settings. If an unmounted partition has no mount directory, it is not be listed. If the Media Server is recording archives, check the check box for at least one Local Archive Repository must be selected. (The archive directory permissions must be set to 777 if owned by root or 755 if owned by nobody. Make these configuration in the Linux operating system. To designate that partition as available for Media Server storage repositories, check the checkbox next to each partition mount.
Clipping	
Local BWM/X Clip Repository	Defines where BWM and BWX clips are stored on the VSMS host. From the Local BWM/X Clip Repository drop-down list, choose the local Media Server repository mount location where BWM are BWX clips stored. Only one mount can be recognized. If **-- No Repository --** is specified, BWM and BWX clip generation fails.

Table 10-7 Media Server Configuration Page Options (continued)

Option	Description
Back-up	
Back-up Repository	List of partitions where backup video archives can be stored. If this VSMS host is to be used as a backup server for video archives, designate each partition that should be available as a storage repository by checking the **Back-up Repository** check box next to the partition mount. A backup server is a VSMS host that is used as a resource to store backup video archives. VSMS can recognize up to 500 partition mounts. Repositories that appear in red type are unmounted locations. This 500 partition mount limit includes the partitions specified in the Local BWM/X Repository configuration settings. If an unmounted partition has no mount directory, it is not listed.
Events	
Maximum Event Marking Duration	The maximum duration for a motion or other event recording. This option should be set to the maximum number of seconds of continuous activity that any camera in a deployment might capture. Valid values are integers 1 through 86400. The default value is 7200 (2 hours).

Media Server Backup Page

The Media Server Backup page lets you create and store a backup file that contains Media Server configuration information. The backup file is a zip file that you can store on your local PC. Then, if necessary, you can use this file to restore the Media Server to a previous state. (If you need to restore the Media Server, contact the TAC for assistance.)

To display the Media Server Backup page, click the **Media Server Backup** link under Configuration at the left side of the Management Console.

To back up the current Media Server configuration, click the **Download Now** button, then use the Save As pop-up window to save the configuration file.

Operations Manager Configuration Page

The Operations Manager Configuration page provide information about VSOM settings and provides options for configuring several basic parameters.

To display the Operations Manager Configuration page, click the **Operations Manager** link under Configuration at the left side of the Management Console.

If you change any options in the Operations Manager Configuration page, you must click the **Update** button at the bottom of the page to save the changes. To discard the changes, exit the page by choosing another page or exiting the browser.

To update options to their last-saved values, click the **Reset** button, then click the **Update** button to save the changes.

Table 10-8 describes the options in the Operations Manager Configuration page.

Table 10-8 Operations Manager Configuration Page Options

Option	Description
Log Level	
Log Level	Use the log level to determine the type of information that the system writes to the VSOM log file. This log file is named vsom.log and is stored on the local host in the usr/BWhttpd/logs/ folder. Log levels are: • **Emergency Only**—Messages related to critical errors that prevent the system from running. • **Error Conditions**—Messages related to any errors that the application experiences. Also includes Emergency Only messages. • **Notice (Default)**—Messages regarding normal actions taken by the application. Also includes Error Conditions and Emergency Only messages. • **Debug**—Debugging information. Also includes messages from all other log levels. The **Emergency Only** log level provides the best performance. The **Debug** log level captures the most data but may cause the system to run slower. Any change that you make to the log level takes effect immediately after you click the **Update** button.
Database Connection	
Database Type	Choose the type of database that VSOM uses to operate. Database types are: • **MySQL 5.0**—Default database type. Specifies that storage uses a local or remote MySQL 5.0 database • **Oracle 10g**—For legacy use. Not supported.
Database Server	Enter the connection location of the database. For MySQL 5.0, enter the IP address of the MySQL server. Use either **localhost** (default) or a fully-qualified IP address.
Database Username	Enter the log in user name that is required for connecting to the database. This name must start with a letter and contain letters and numbers only. It is case sensitive. This value should be changed only if configuring an advanced deployment on a shared MySQL server. The default user name for MySQL is **cisco**.

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
Database Password	Enter the log in password that is required for connecting to the database. This name can contain any combination of up to 41 letters and numbers. This value should be changed only if configuring an advanced deployment on a shared MySQL server. The default password is **mysql**. **Note** Changing this Database Password does not change your database user password. You must change your user password in the database before you change this Database Password.
Database Name	Typically database servers allow multiple schemas or database instances. The Database Name points to the correct schema or instance on the database server. MySQL—The pre-determined database name used by the application. The default username is cisco. This value should be changed only if you are using a database other than MySQL or configuring an advanced deployment on a shared MySQL server. The default value is BAS.
Database Configuration Validation	
Database Status	Click the **Validate DB** button to check the database connection status and verify that database tables were created correctly. These checks are based on the database settings that were configured when you last clicked the **Update** button on this page. The validate function checks table names only. It does not validate the database schema. Information appears in a pop-up window. Click **OK** to close the window.
SMTP Parameters	
SMTP Server	Enter the IP address of host name of an SMTP server to which the system routes e-mail that the application generates when an event occurs.
SMTP “From:” Address	Enter an e-mail address to a appear in the From: field of e-mails that the system sends. This field is required if VSOM is to sending e-mail message when an SNMP event occurs.

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
User Login Authentication	
Authentication Type	Choose how the system validates a user name and password that a user enters when logging in to VSOM. Authentication types are: • **Application Database**—Default selection. Designates that VSOM authenticates a user name and password against its internal database. • **LDAP Server**—Designates that VSOM authenticates a user name and password against the LDAP server that is configured in the LDAP Configuration section. When using an LDAP Server, the users must be manually created in VSOM, and the user name must match exactly the user name that is configured in the authenticating LDAP server.
LDAP Configuration **Note** These fields are required only if you choose **LDAP Server** from the Authentication Type drop-down list. If you choose **Application Database** from that list, these fields are ignored and can be left empty.	
Host Name	Enter the IP address or the host name of the LDAP server to be used to authenticate user log in credentials. For example, ds.cisco.com.
Host Port	Enter the port number of the LDAP server that is used to authenticate user log in credentials. If this field is blank, the value 389 is used.
Relative Distinguished Names (RDN)	Enter the LDAP Relative Distinguished Names to be used for authentication. In the RDN, the token %username% is replaced dynamically with the user name when a user attempts to log in. For example, enter: CN=%username%,OU=Employees,OU=cisco users
Domain Controllers (DC)	Enter the list of domain controllers, in order of precedence. Separate each controller with a semicolon (;). For example, enter: DC=amer,DC=cisco,DC=com;DC=euro,DC=cisco,DC=com
Delimiter	Enter a character to use as a delimiter between the RDN and the DC. The default delimiter is a semicolon (;).

Table 10-8 Operations Manager Configuration Page Options (continued)

Option	Description
Select Homepage	
Change default homepage to VSOM Change default homepage to VSMC	Click a radio button to designate the action that the system takes when you access a VSOM or VSMS server with the following address and then log in. (<*server*> is the IP address or hostname of the server.) http://<*server*> • **Change default homepage to VSOM**—The system displays the VSOM login page. If you do not select this option, you enter **http://<*server*>/vsom** to access the VSOM Log In page, where <*server*> is the IP address or hostname of the VSOM server. • **Change default homepage to VSMC**—Displays the Management Console. If you do not select this option, a user must enter http:**//<*server*>/vsmc.html** to open the Management Console, where <*server*> is the IP address or hostname of the VSMC host.

Operations Manager Backup Page

The Operations Manager Backup page lets you create and store a backup file that contains VSOM configuration information and a copy of the local VSOM database. The backup file is a zip file that you can store on your local PC. Then, if necessary, you can use this file to restore VSOM to a previous state. For information about restoring, see the "Restore the database" instructions in Table 4-2 on page 4-3.

To display the Operations Manager Backup page, click the **Operations Manager Backup** link under Configuration at the left side of the Management Console.

To back up the current VSOM configuration, follow these steps:

Procedure

Step 1 Click the **Operations Manager Backup** link under Configuration at the left side of the Management Console.

The Operations Manager Backup page appears.

Step 2 In the MySQL root password field, enter the MySQL root user password.

The system requires this password so that the SQL database can be backed up. If you provide an invalid password, the backup completes, but the SQL dump inside the resulting .tar does not contain the VSOM data.

Step 3 Click the **Download Now** button, then use the Save As pop-up window to save the configuration file.

Virtual Matrix Configuration Page

The Virtual Matrix Configuration page lets you designate the port number on a Video Surveillance Virtual Matrix (VSVM) host that VSOM uses to communicate with that host. (Cisco suggests that you consult with the TAC before changing this port number.)

To display the Virtual Matrix Configuration page, click the **Virtual Matrix** link under Configuration at the left side of the Management Console.

To change the VSVM host port number that VSOM uses to communicate with this host, follow these steps:

Procedure

Step 1 Click the **Virtual Matrix** link under Configuration at the left side of the Management Console.

The Virtual Matrix Configuration page appears.

Step 2 In the Server Port field, enter the port to use.

Valid values are integers from 1024 to 65535. The default port number is 8086.

Step 3 Click **Update** at the bottom to save the changes.

If you want to discard the change, exit the page by choose another page or exiting the browser.

Note If you want to set the Server Port value to its previously-saved value, click **Reset** and then click **Update**.

Step 4 Restart the VSVM server as described in the "Restart Server Page" section on page 10-28.

Management Console Password Page

The Management Console Password page lets you designate the password that must be entered to access the Management Console.

For security, Cisco recommends that you change the default system password immediately after installing the system, and that you continue to change the password regularly.

To display the Management Console Password page, click the **Console Password** link under Configuration at the left side of the Management Console.

To designate the management console password, perform the following steps.

Note After you change the password, the Management Console prompts for the new password before it displays another page.

Procedure

Step 1 Click the **Console Password** link under Configuration at the left side of the Management Console.

The Management Console Password page appears. The User Name field indicates that the user name for logging in to the Management Console is **root**.

Step 2 In the New Password field, enter a password that adheres to these guidelines:

- Minimum length—3 characters
- Maximum length—10 characters
- Valid characters—Upper case letters, lower case letters, and numbers

The password is case-sensitive.

Step 3 In the Confirm New Password field, enter the password again.

The entry in this field must match exactly the entry in the New Password field.

Step 4 Click **Update** to implement the new password.

Camera Firmware Upgrade Page

The Camera Firmware Upgrade page lets you upgrade the firmware in the video cameras in your deployment. When you use the upgrade camera firmware feature, be aware of these guidelines:

- This feature is available only if VSMS is installed of your system.
- Do not perform the camera upgrade procedure when a server upgrade is in process because doing so may cause the camera upgrade to fail. (If you open the Camera Firmware Upgrade page while a server upgrade is in process, an alert message informs you that the server upgrade is in process.)
- You can execute an upgrade for one camera or for multiple cameras. You can rerun the upgrade procedure as needed to upgrade cameras of the other type.
- When upgrading Cisco IP camera models 2911, 2916, 2930, 2935, 5010, or 5111, be aware that each camera includes a firmware file that is specific to the model. The camera firmware upgrade process displays the camera model family (for example, 29xx or 5xxx), not the specific model. You must determine the specific camera model before upgrading a camera. If an incorrect firmware file is used, the upgrade process fails.
- If you will use the Cisco video analytics feature on Cisco HD IP Camera 4500 model that is running a firmware version lower than 1.2.1, you must first upgrade the camera to firmware version 1.2.1, then upgrade the camera to a firmware version that provides support for the video analytics feature.
- The upgrade process can take approximately 10 minutes for each camera. If you choose to upgrade multiple cameras, they are upgraded one at a time, in the order that you selected them. A camera is not operational while it is upgrading. Cisco recommends that you perform this process during off-peak hours.
- While the upgrade process is running, you can perform other operations from the Management Console or with VSOM.
- If you are upgrading multiple cameras and a fatal error occurs while upgrading one of them, the upgrade process stops and no additional cameras are upgraded. If a non-fatal error occurs, the camera that experiences the error is not upgraded, but the upgrade process continues for the remaining cameras. Fatal errors includes a camera not coming back on-line after an upgrade or a camera failure during the upgrade. Non-fatal errors include invalid camera log-in credentials.

Note Upgrading your version of Cisco VSM may require you to update the firmware in the cameras in your VSM deployment. See the camera firmware release notes to determine if a camera firmware upgrade is required.

Upgrading a camera is a two-part process: First, obtain the firmware from Cisco.com. Then, use the Camera Firmware Upgrade page to perform the upgrade. To upgrade camera firmware, follow these steps:

Procedure

Step 1 Obtain the desired camera firmware package by going to the following URL and downloading the package to your local PC, a network PC, or an FTP server:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=280249565

The firmware package is in a zip file.

Step 2 Start the Management Console and click the **Camera Firmware Upgrade** link under Configuration at the left side of the Management Console.

The Camera Firmware Upgrade page appears.

Step 3 From the Camera Firmware Type drop-down list, choose the Cisco IP camera series to which the camera or cameras that you want to upgrade belongs.

In the options that appear in this list, "SD" indicates standard definition and "HD" indicates high definition. For example, the option **Cisco SD 25xx** indicates the Cisco Video Surveillance 25xx series IP camera models.

A list of cameras that you have deployed and that are in the camera series that you choose appears.

Step 4 In the list of cameras, check the check box next to each camera that you want to upgrade, or check the check box at the top of the list to choose all cameras.

If you choose multiple cameras, these cameras upgraded one at a time in the order that you choose them. If you choose all cameras, they are upgraded one at a time in the order that they appear in this list.

Each item in this list includes the following information:

- Camera Name—Name that VSMS assigned to the camera. This name is based on the camera name that is configured in VSOM, with underscores (_) and some extra text removed.
- Model—Cisco model number of the IP camera
- IP/Hostname—IP address of host name of the IP camera
- Version—Firmware version that is installed on the IP camera. The "Unknown" designation indicates a camera that has not responded to a request from VSMS for its firmware version, or for which VSMS cannot determine the firmware version for some other reason. A camera with this designation may not be able to upgrade.

You sort this list by any column in ascending or descending alphanumeric order. To do so, click a column name to toggle between ascending or descending order, or choose the desired order from the drop-down list that appears when you mouse over a column name.

To make sure that this list shows current camera version information, click the **Refresh Cameras** button.

Step 5 Take one of these actions to identify the firmware package to use for the upgrade:

- If the firmware package is on your local disk or a network disk, click the **File Upload** radio button, then enter the path and file name of the firmware package in the **Upgrade file from cisco.com** field. You can use the **Browse** button to locate the firmware package.
- If the firmware package is on an FTP server, click the **FTP Download** button and take these actions:
  - In the FTP Server field, enter the name of the FTP server

- In the Path on FTP Server field, enter the full FTP server path name relative to the home directory of the FTP account, and file name for the firmware upgrade package. Use the format */file_name*, where *file_name* is the name of the firmware package.
- FTP User Name—User name that you use to log in to the FTP server
- FTP Password—Password that you use to log in to the FTP server.

Step 6 Click **Start Upgrade**.

The system performs that upgrade. If you chose multiple cameras, they upgrade in the order that you chose them. If you chose all cameras, they are upgraded one at a time in the order that they are listed on the Camera Firmware Upgrade page.

A status panel displays the progress of the upgrade. Detailed status messages appear in the scrollable text area and general status appears in the status bar.

In addition, the system stores information about the upgrade in the following log files. Refer to the log files if an error occurs during an upgrade. You can use a text editor to view these files. If you want to save them, change their names or move them to another folder, because the system overwrites them each time you perform an upgrade.

- /usr/BWhttpd/upgrade/endpoint/endpoint_upgrade.log—Detailed upgrade log
- /usr/BWhttpd/upgrade/endpoint/endpoint_upgradesummary.log—Upgrade summary

You can abort the upgrade process by clicking the **Cancel Upgrade** button and then click OK in the confirmation pop-up window. If you are upgrading multiple cameras, you can stop the upgrade procedure clicking the **Cancel Upgrade** button. When you click this button, the upgrade that is in process for a camera completes, which can up to approximately 10 minutes, but no additional cameras are upgraded.

Server Upgrade Page

The Server Upgrade page lets you upgrade the VSMS software that is running on the VSMS host. When you use the upgrade server feature, be aware of these guidelines:

- This process upgrades VSMS only. To upgrade VSOM, see the *Installing and Upgrading Cisco Video Surveillance Manager Release 6.3.1* document.
- The server upgrade page is available only if VSMS is installed of your system.
- This feature allows upgrading from VSMS 6.3.0 or later. It does not support earlier releases.
- Do not perform the server upgrade procedure when a camera upgrade is in process because doing so may cause the camera upgrade to fail. (If you open the Server Firmware Upgrade page while a camera upgrade is in process, an pop-up message informs you that the camera upgrade is in process.)
- The upgrade process can take approximately 20 minutes. During this time, your VSM system is not operational. Cisco recommends that you perform this process during off-peak hours.
- The upgrade process automatically restarts the VSMS host.
- After the upgrade process completes, you can manually delete the files in the /usr/BWhttpd/upgrade/server/download folder.
- If you upgrade VSMS on a host on which VSOM is also installed, Cisco recommends that you also upgrade VSOM on that host. For instructions, see *Installing and Upgrading Cisco Video Surveillance Manager (VSM)*.

Upgrading VSMS software is a two-part process: First, obtain the software from Cisco.com. Then, use the Upgrade Server page to perform the upgrade.

To upgrade the VSMS software, follow these steps:

Procedure

Step 1 To obtain the new software upgrade package, from any PC, go to this URL and download the package to an FTP server:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281550158

The software upgrade package is in a zip file.

Step 2 Start the Management Console and click the **Server Upgrade** link under Configuration at the left side of the Management Console.

The Management Upgrade Server page appears.

Step 3 Take one of these actions to identify the software upgrade package to use for the upgrade:

- If the software upgrade package is on your local disk or a network disk, click the **File Upload** radio button, then enter the path and file name of the software package in the **Upgrade file from cisco.com** field. You can use the **Browse** button to locate the software package.
- If the software upgrade package is on an FTP server, click the **FTP Download** button and take these actions:
  - In the FTP Server field, enter the name of the FTP server
  - In the Path on FTP Server field, enter the full FTP server path name relative to the home directory of the FTP account and file name for the software upgrade package. Use the format */file_name*, where *file_name* is the name of the software package.
  - FTP User Name—User name that you use to log in to the FTP server
  - FTP Password—Password that you use to log in to the FTP server.

Step 4 Click **Start Upgrade**.

The system performs the upgrade. When the upgrade completes, the system restarts automatically.

A status panel displays the progress of the upgrade. Detailed status messages appear in the scrollable text area and general status appears in the status bar.

In addition, the system stores information about the upgrade in this log file: /usr/BWhttpd/upgrade/server/upgrade_progress.log. Refer to this file if an error occurs during an upgrade. You can use a text editor to view this file. If you want to save this file, change its name or move it to another folder, because the system overwrites it each time you perform an upgrade.

Restart Server Page

The Restart Server page lets you restart the VSM software on the host that you are accessing. The option on this page does not reboot the host on which the software is running.

The VSM software should be restarted after a Media Server configuration change or a VSMS restore.

To restart the server that you are accessing, click the **Restart Media Server** button on the Restart Media Server page. The restart process starts and messages about the process appear in the bottom area of the page. A success message appears when the server has restarted.

Reboot Server Page

The Reboot Server page lets you reboot the VSM server that you are accessing.

To reboot the server, click the **Reboot Media Server** button on the Reboot Media Server page. The reboot process starts and messages about the process appear in the bottom area of the page. A success message appears when the server has rebooted.

Shutdown Server Page

The Shutdown Server page lets you shut down the VSM server that you are accessing.

To shut down the server, click the **Shutdown Media Server** button on the Shutdown Media Server page.

Other Utilities

The Management Console provides the following pages for accessing related do documentation and preparing a report for troubleshooting:

- Media Server User Guide—Displays an on line version of *Cisco Video Surveillance Media Server User Guide*. The document displays in a window that includes links and tools for navigating through the document and locating desired information.
- Server Report—Creates and saves a report that contains VSM logs and configuration information, and server logs and configuration information. The report is stored as a zip file and can be provided to the Cisco Technical Assistance Center (upon request).

  To create a support report, click the **Generate** button, then use the Save File pop-up window to save the report. It can take several minutes to process the report. Do not navigate away from or refresh this page until you see the Save File pop-up window.