Securing Cisco Video Surveillance Manager 4.1/6.1: Best Practices and Recommendations

This document provides best practices and recommendations for helping to ensure the security of Cisco Video Surveillance Manager (VSM) 4.1/6.1 components in a video surveillance deployment. These components include Cisco Video Surveillance Operations Manager (VSOM), Cisco Video Surveillance Media Server (VSMS), 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.

These guidelines can be 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:

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

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 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 VSM serves. However, its 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 VSMS and administrative users only.
- On network switches, configure access lists to allow Cisco VSMS 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 access a system.

Passwords to change include the following:

- Video Surveillance Management Console (VSMC) password
- VSOM user “root” password
- Linux user “root” password

Procedures for configuring these passwords follow.

Changing the Video Surveillance Management Console (VSMC) password

Step 1 Access the VSMC page on the server on which you want to change the password.

Step 2 Click the **Console Password** link.

Step 3 Enter and confirm the new password.

Step 4 Click **Update**.

Changing the VSOM user “root” password

Step 1 Log in to VSOM as the user “root.”

Step 2 Click the **Preferences** icon to configure user preferences.

Step 3 Click the **Change Password** button.

Step 4 Enter the current password, and enter and confirm the new password.

Step 5 Click **Submit**.

Changing the Linux user “root” password

Step 1 Log in to the server console as the user “root.”

Step 2 Enter the following command:

shell> **passwd**

The system displays: `Changing password for root.`

Step 3 Respond to the following prompts, replacing *new_password* with the password that you want to set:

New Password: ***new_password***

Reenter New Password: ***new_password***

Note For more information, enter the **man passwd** command on the Linux command line.

s

Configuring the MySQL User “root” Password

It is a best practice to set a MySQL user “root” password. MySQL “root” has no password by default. Not setting this password may allow an unauthorized user to read, modify, or delete VSM configuration information.

To set this password, perform the following steps. See your MySQL documentation for more information.

Step 1 Log in to the server console as the user “root.”

Step 2 Enter the following command:

shell> **mysql -u root**

The command prompt changes to mysql.

Step 3 Enter the following commands, replacing *new_password* with the password that you want to set:

mysql> **SET PASSWORD FOR ''@'localhost' = PASSWORD(“*new_password*”);**

mysql> **SET PASSWORD FOR ''@'%' = PASSWORD(“*new_password*”);**

Configuring a Firewall for Cisco VSM

VSM hardware ships with 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.

Table 1 shows the firewall ports that may need to be open, depending on your video surveillance deployment and components.

Table 1 Firewall Ports that VSM May Use

Port	Use
TCP ports	
22	SSH[1]
80	VSMS, VSOM
443	VSOM
554	VSMS
1066	VSVM[2]
8086	VSVM
UDP ports	
123	NTP[3]
1024:1999	Panasonic, Pelco, Sony devices
6000:6999	Cisco, ACTi, VCS (Bosch) devices
16100:16999	Axis, Teleste devices

Table 1 Firewall Ports that VSM May Use (continued)

Port	Use
18000:18999	Vbrick devices
20000:20999	Mango devices
55000:55999	Optelecom

1. SSH = Secure Shell.
2. VSVM = Cisco Video Surveillance Virtual Matrix
3. NTP = Network Time Protocol.

Using Secure Remote Access

To access VSM servers remotely, use SSH instead of Telnet and SFTP instead of FTP. SSH and SFTP provide additional security. Using an nonsecure remote access method puts your communication at risk to be accessed and read.

Session Timeouts

In VSOM, 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.

In addition, set the Linux command line bash shell timeout period as follows:

Step 1 Log in to the server console as the user for whom you want to change the session timeout period.

Step 2 Edit the ~/.bashrc file and add the following line to this file to set a shell session timeout for the user:

```
export $TMOUT=<seconds>
```

Replace <*seconds*> with the number of seconds that the command line remains idle before it times out.

Locking Down Requests for VSM

You can restrict VSMS from accepting certain requests (configuration commands, information queries, and video streams) by locking down the operations that you want to protect. You can also authorize VSMS to accept requests only from designated IP addresses of servers and clients. Locking down request help reduce the risk of disruption to video recording or monitoring, and unauthorized updates to system configuration.

If VSMS receives a locked-down request, it rejects the request and generates the status code “403 Access Denied.”

There are two text files in VSMS that let you manage locked-down requests and authorized IP addresses:

- The .locked.cmds file in the /usr/BWhttpd/conf folder—Contains a list of request strings that are locked down.
- The .locked.addrs file in the /usr/BWhttpd/conf folder—Contains a list of IP addresses of the servers and clients that are authorized to issue locked down requests to VSMS.

As a best practice, perform this procedure so that only one designated VSOM can manage the configuration of VSMS:

Step 1 Use a text editor to open the /usr/BWhttpd/conf/.locked.cmds file.

Step 2 In the .locked.cmds file, enter the following lines:

```
/cgi-bin/smanager.bwt?*command=save
/cgi-bin/smanager.bwt?*command=remove
/command.bwt
/event.bwt?*command=setup
/event.bwt?*command=event*type=stop
/event.bwt?*command=enable
/event.bwt?*command=disable
/archive_backup
```

Step 3 Save the file.

Step 4 Use a text editor to open the /usr/BWhttpd/conf/.locked.addrs file.

Step 5 In the .locked.addrs file, enter the IP address of the VSOM server.

Step 6 Save the file.

Step 7 Use the following command to restart VSMS:

/etc/init.d/cisco restart

If you want to make other updates to the .locked.cmds file or the .locked.addrs file, follow these guidelines:

- Use a text editor to open the desired file.
- When saving an updated file, do not change its name or permissions.
- In the .locked.cmds file:
  - Enter one request string to be locked down per line. Do not enter any other text in the file.
  - A request string can contain one or more of the wildcard *, each of which matches any character string of any length. For example, the command info.bwt*type=sdp matches any command that includes info.bwt followed by type=sdp later in the command.
  - When entering a query string with more than one argument, the arguments must be entered in the order in which the requestor provides them. If you do not know this order, specify the arguments in all possible variations by entering the query string multiple times.
  - To optionally designate one or more server or client from which VSMS accepts locked down requests, follow the request string with two colons (::) and the IP addresses of each server or client. If you include more than one IP address, separate each address with a coma. For example, info.bwt::10.10.50.4,10.10.50.6 designates that VSMS accepts the info.bwt request only from servers and clients with the IP address 10.10.50.4 or 10.10.50.6.
  - If you enter only * on a line, all requests are locked down.
- In the .locked.addrs file:
  - Enter one IP address per line.
  - Do not enter any other text in the file.
- After saving a file, restart VSMS by running the following command:

  /etc/init.d/cisco restart

If no IP addresses are specified in the .locked.addrs file, or if this file does not exist, VSMS accepts requests only from servers or clients with IP addresses that are designated in the .locked.cmds file. If the locked.addrs file is empty or does not exist, and any command .locked.cmds file does not have associated IP addresses, VSMS cannot accept those requests.

Note If you are using servers that are not provided by Cisco, you must install the VSMS package with VSOM to be able to use the lockdown feature.

Table 2 lists the operations that you can lock down in the format that they should appear in the .locked.cmds file. At a minimum, Cisco recommends that you lock down the handlers that are indicated in the Recommended for Lock Down column, because these handlers can affect the configuration of the system.

Table 2 Operations to Lock Down

Operation Request String	Purpose	Recommended for Lock Down
Command Handlers		
/cgi-bin/smanager.bwt?*command=save	Clipping	Yes
/cgi-bin/smanager.bwt?*command=remove	Remove archive	Yes
/command.bwt	Management of live and recorded video	Yes
/archive_backup	Initiates and configures archive backup	Yes
/event.bwt?*command=setup	Create event profile	Yes
/event.bwt?*command=event*type=stop	Stop event clip	Yes
/event.bwt?*command=enable	Enable event	Yes
/event.bwt?*command=disable	Disable event	Yes
/event.bwt?command=event*name=	Trigger event profile	
Stream Handlers		
/video.jpeg	Live JPEG streams and thumbnail image preview	
/media.bwt	Live MPEG-4 streams	
/stream.bwt	Live MPEG-2 streams	
/ondemand.bwt	Archives (all media types)	
/audio.bwt	Live audio streams	
Read-Only Information Handlers		
/info.bwt[1]	VSMS status information	
/event.bwt?*command=event*property=setup	List event profiles	
/cgi-bin/smanager.bwt?*command=DiskUsage	List disk use for repositories	

1. The info.bwt handler is required by client systems to render video. It also is required by any applications, including VSOM, that interact with VSMS.

Configuring User-Based Authentication

As a best practice, use an Apache .htaccess file to provide user-authenticated access to directories on Cisco VSMS.

Cisco recommends that you restrict access for the following VSM web directories that Table 3 describes:

Table 3 VSM Web Directories for Restricted Access

File	Description
/BWT /files	Contains the software developer kit interface, which is not required for typical system operation
/doc	Contains VSM technical documentation
/download	Stores support information that is generated for submission to Cisco support

See your Apache documentation for additional information about the .htaccess file.

Linux Host User Administration

Create local users with administrative privileges on the VSM servers, then use the **sudo** command to run commands as the root user. This process provides a user-specific audit trail by tracking and logging administrator access and activity on the system.

See your **sudo** command documentation for more information.

VSOM User Administration

Create users and roles in VSOM and use these login credentials instead of logging in as root. This process provides a user-specific audit trail by tracking and logging administrator access and activity on the system. Without users and roles, you cannot identify who performs various activities, which may allow an unidentified user to disrupt your system.

Enabling VSOM Secure Login

Configure the Enable Secure Login feature in Cisco VSOM. This feature encrypts login credentials when users log in to VSOM. Unencrypted login credentials can be captured over a network.

Logging Out from Management Console and VSOM

As a best practice, always log out and close the browser when you leave a VSOM session.

In addition, always close your browser when you complete a Management Console session.

Logging out and closing the browser 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.