Design and Development Smart Classroom for Lecturing Video Capture

Zhi-Xue Xu, San Jose State University
Design and Development Smart Classroom for Lecturing Video Capture

1. General

2. Video Endpoint for Lecture Video Capture

   2.1 Basic connections and Physical Interface in Cisco C90

      2.1.1 Video Ports (Input and Output)
      2.1.2 Audio Ports (Input and Output)
      2.1.3 Audio from PC (Line in)

   2.2 Web Interface for full configuration in Cisco C90

      2.2.1 The interactive menu
      2.2.2 Diagnostics
      2.2.3 Configuration
      2.2.4 Call Control by users
      2.2.5 Maintenance

3. Content Server for Video and Lecture Capture

   3.1 Introduction to Video Content Server

   3.2 Cisco TelePresence Content Server (TCS)

      3.2.1 Hardware and Software Installations of Cisco Content Server
      3.2.2 Configuration of Cisco Content Server
      3.2.3 Using Cisco Telepresence Content Server
         I. The View Recordings
         II. The My Recordings
         III. Recordings Aliases
         IV. Distribution Outputs

4. Media Experience Engine for Lecture Video Capture Control

   4.1 Installations of Cisco MXE 3500
   4.2 Configuration of Cisco MXE 3500

      4.2.1 Work Steps of Configuring the Host Settings
      4.2.2 Work steps of Configuring the Input and Output Media Directories
      4.2.3 Work steps of Configuring User Settings
4.2.4 Configuring the Video Conversion Interface (SUI)
4.2.5 Configuring Shared Folders

4.3 Using Cisco MXE 3500 Web User Interface

4.3.1 Accessing the Cisco MXE 3500 Web UI
4.3.2 Information Panel
4.3.3 Menu Bar
4.3.4 Toolbox
4.3.5 Profile Browser
4.3.6 4.3.6 Main Window

5. Show and Share for Video Lecture Capture

5.1 Installation for Cisco Show and Share and Digital Media Manager Release 5.3.10 on the Cisco MXA UCS M3 Server

- Hardware Installation of Cisco MXA UCS M3 Server
- Initial Server Setting up and Installing the Cisco MXA UCS M3

5.2 Using Cisco Show and Share

- Access Cisco Show and Share
- Sign In to Cisco Show and Share
- Access the Administration Area
- User Roles and Privileges
- Show and Share Home
- Video Playback
- My Account
- Upload Video
- Record a Video
- Publish Your Video

5.3 Using Cisco Digital Media Manager (DMM)

- Start Digital Media Manager (DMM)
- DMS-Admin Dashboard
- Check Processes Remotely
- Allow or Disallow Video Transcoding
- Users and Groups

5.4 Show and Share for Video Lecture Capture from Vyopta
• Using Vyopta vControl and vPublish in Smart Classroom
• Using Show and Share in the Smart Classroom
Design and Development Smart Classroom for Lecturing Video Capture

Zhi-Xue Xu  
Academic Technology  
San Jose State University  
May 29, 2014

1. General

Design and Development Smart Classroom for Lecture Video Capture is one of the important next generation technologies for Smart Classroom in Academic Technology. Lecture Video Capture has been applied to high education and distance learning. San Jose State University is going to use Video Capture Technology creating 51 Smart Classrooms on campus to provide success learning spaces for High Education, eCampus, and eLearning. The members of Faculty can record their lectures in the smart classroom, and live video streaming web broadcast. Through the Video Content Server and Sharing, students can watch the lecture repeatedly with the permit from the lectures. These Lecture Video Captures can be applied to eCampus and distance learning too.

There are three important sections in Design and Development Smart Classroom for Lecturing Video Capture. The three sections included Endpoint with Camera and Microphone, and Video Content Server for capture, Transform and show and share. Cisco has developed the equipment and hardware with software that included Video Codec, Content Server, Media Experience Engine, and show and share for Video Capture to High Education in the classrooms. Cisco Technology Partner Vyopta also provided the software for the Video Content Management, vControl and vPublish. Adobe also had applied Flash Video Server 5 for codec video streaming and content server with Linux and Windows Servers to High Education on campus.

The general concept of Design and Development Smart Classroom for Lecturing Video Capture is the following:

- **Endpoint**: The Endpoint included Camera and Microphone, and Video Content Server for capture. The video capture can be recording to Content Server in Windows, Mac and Linux computer servers. Cisco has provided Cisco codec C40 and C90 for Endpoint.

- **Transform**: We need a Media Experience Engine that can be built in Windows, Mac and Linux computer servers, can be integrated content server together. The Web Server and Database in the Media Experience Engine will be used to Live Web Video Broadcasting and Show and Share. Cisco can provide Media Experience Engine: Cisco MXE 3500.

- **Show and Share**: The Show and Share is a Web software application. Cisco has developed this Show and Share Software for much equipment that also can be
integrated to Cisco MXE 3500. We can also use Youtube, Vimeo, 56.com and so on to video Show and Share.

General Concept of Design and Development for Video Lecture capture in the Smart Classroom

1. End point:

![Diagram of End point]

2. Transform:

![Diagram of Transform]

3. Show and Share

![Diagram of Show and Share]

Fig. 1 General Concept of Design and Development Smart Classroom for Lecturing Video Capture
We believe that the Video Capture Technology will be wide to use in the classrooms and
distance learning for High Education in the future, and create and provide new and advanced
reforms of High Education. Video Capture Applications for High Education is a great challenge to
the current education systems. Video Lecture Capture will be important topic and project in
Academic Technology.

We will provide concept, samples, work steps and information of the equipment for
Design and Development Smart Classroom for Lecturing Video Capture.

2. Video Endpoint for Lecture Video Capture

There are three important hardware components in Video Endpoint for Lecture Video Capture. The
endpoint hardware components included Camera, Microphone and Monitors. We also need the
software for the hardware components to video recording to Content Server and Live Web Streaming
Broadcasting by Web Server. It is enough resolution for Lecture Video Capture that you can use cheaper
Camera, Microphone and Monitors. We can develop the software, and use the open sources for video
content server and web server to video web broadcasting for show and share by the lower cost.

Cisco TelePresence System Codec C90 has been applied to the Next Generation Classrooms as Smart
Classrooms in San Jose State University.

Fig. 2.1 Next Generation Classrooms as Smart Classrooms in San Jose State University
2.1 Basic connections and Physical Interface in Cisco C90

The interface of Cisco TelePresence System Codec C90 included video ports, audio ports and network Ethernet port. These ports will connect to Monitors, Cameras, Microphones, Speakers, PC and network. The information of introductions about video and audio ports, and network Ethernet port is the following:

![Physical Interface in Cisco C90](image)

**Fig. 2.2 Physical Interface in Cisco C90**

2.1.1 Video Ports (Input and Output)

- Monitors (HDMI 1 and HDMI 3)

- Main Camera and Second Camera (HDMI1 and HDMI 2)

![Camera in Cisco C90](image)

**Fig. 2.3 Camera in Cisco C90**

- Camera control (Com port)
- Video from PC (DVH 3)
2.1.2 Audio Ports (Input and Output)

- Audio Input: Microphones
- Audio Output: Speakers (Line out)

Fig. 2.4 Speakers

- Audio from PC (Line in)

2.1.3 Network Ethernet port

2.2 Web Interface for full configuration in Cisco C90

The web interface provides full configuration access to the video conference system. We can connect from a computer and administer the system remotely.
Fig. 2.5 Log in to Web Interface

We can be using the web interface for system configuration and maintenance.

2.2.1 The interactive menu

Fig. 2.6 Main Menu in Web Interface
The web interface provides access to tasks and configurations. They are available from the main menu. The main menu appears near the top of the page when you have signed in. The main menu included four sections: Diagnostics, Configuration, call control and Maintenance. Three user roles are defined: Admin, Audit and User.

2.2.2 Diagnostics

Diagnostics have three sections: System Information, Log Files and XML Files. Click **System Information** under Diagnostics. You will get System Information as follows:

![System Information](image)

*Fig. 2.7 System Information in Web Interface*

The System Information includes System Name, Product type, software version, IP address, recent login, etc.

**Log Files**

Click the Log Files. You can get a list of log files:
Fig. 2.8 Log files in System Information

The log files are Cisco specific debug files if you need technical support. The log files are time stamped event log files.
XML Files

There are four XML file in System Information: Configuration, Status, command and valuespace.

2.2.3 Configuration

Configuration has three sections: Advanced Configuration, Wallpaper and Sign in Banner.

Click Advanced Configuration under configuration, and get a System setting:
The system settings are grouped in several categories. When we select a category in the left column, all related settings appear in the window to the right.

**Selecting a Wallpaper**

We can select between a set of predefined wallpapers as background on the display.
Fig. 2.11 Wallpaper in configuration

**Sign in Banner**

If a system administrator wants to provide initial information to all users, he can create a sign in banner. A sign in banner is message that is displayed to the user before signing in.
Fig. 2.12 Sign in Banner

The message will be shown when the user signs in to the web interface or the command line interface.

2.2.4 Call Control by users

Placing a call

We can use the call control page of the web interface to initiate a call Controlling and monitoring a call. You can call one by entering one or more characters in the address input field until the name you want to call appear in the dynamic search list. Or, enter the complete email address, then press Dial and press End all to disconnect the call.

The video system, display, microphone and speakers will be used for the call.
Fig. 2.13 Placing a call
Controlling and monitoring a call

We can control and monitor several call feature by using Call control page. The Call controlling included adjusting the sound volume, Muting the microphone, Controlling the Camera, Call settings, and Call details.

Fig. 2.14 Controlling and monitoring a call
Local layout control

We also can select a local layout by using the Call Control page. Different types of meetings will require different layouts.

Fig. 2.15 Local layout control
Capturing snapshots

Captures from the video system's camera as well as from its presentation channel will be displayed.

The snapshot feature is disabled by default, and must be enabled.

2.2.5 Maintenance

Maintenance has six sections: Software Upgrade, Certificate management, Audit certificate, User Administration, Restart and Factory Reset.
Upgrading the system software

We can initiate software upgrades with release key and option keys.

Fig. 2.17 Upgrading the system software
Certificate management

The SSL certificate may be issued by a certificate authority.

Fig. 2.18 SSL certificate management
Audit certificate

You must upload a list of trusted audit certificates to the video conference system if you want to use the ExternalSecure audit logging mode.

Fig. 2.19 External audit certificate
User Administration

We can manage the user account of the video conference system. We can create new user accounts, edit the details of existing users, and delete users. The default user account is username: admin and no password.

The user roles included admin, user and audit.
**Restarting the system**

Press Restart, we can restart the system. Restarting system will take a few minutes.

Fig. 2.21 Restart the System
Factory Reset

When performing a factory reset the call logs, all files that have been uploaded will be deleted.

Fig. 2.22 Factory Reset

3. Content Server for Video and Lecture Capture

After we set up the Endpoint for the Smart Classroom with cameras and microphone, our video and lecture capture should be recorded to save and transfer in the video content server. The content server has database for video recording. Cisco has provided TelePresence Content Server, which records Cisco TelePresence C40, C60 and C90 Codec and third-party videoconferencing meetings and multimedia presentations for live broadcast and on-demand access.

3.1 Introduction to Video Content Server
The Content Server is a network telepresence media recording, archiving, streaming, and sharing solution.

With the Content Server, those in the organization can get the message across regardless of the day, time, devices, or location. Whether delivering a briefing to an entire organization, facilitating corporate training programs, or offering a distance education course, video recordings are a powerful organizational tool. The Content Server maximizes the impact, reach, and value of these messages by capturing presentations, streaming them live, and recording them for future distribution.

No longer is any message bound by place and time. Recording and streaming telepresence-generated content enables organizations to communicate to dispersed individuals and scale knowledge—anytime, anywhere. Content can integrate easily into familiar third-party tools, extending the reach and chances that your message will be seen and heard. With the Content Server, existing video conferencing investments are fully leveraged, and your messages are viewed by more people more often.

The video content server provides capture video using any device that included smartphone, tablets and desktop, transform the video for optimized viewing on different devices, from mobile devices and PCs to large high-definition displays in the conference room or smart classroom, and share the video with people anywhere in the world and in real time.

Faculty and students can view video any time at their convenience from the content server if they could not attend the class or meeting. The members of faculty and students can view live or archived video from the content server anywhere. The devices to view video from the content server can be any device that included mobile devices, laptops and PCs.

The video content server has become an important tool for distance learning, and it will be easy to provide the courses repeatedly.

3.2 Cisco TelePresence Content Server (TCS)

The Cisco TelePresence Content Server helps us easily record video conference and multimedia presentations for live or on-demand access.

The Cisco TelePresence Content Server allows us to share knowledge and enhance communication by recording video lecture capture in the Smart Classroom. We can access live and on-demand presentations anywhere, anytime. In addition, we can distribute live or recorded content to any computer, or download to the favorite portable media device.

This release introduces the third-generation Content Server hardware that runs Cisco Content Server Release 6.x software. The third-generation Content Server is based on the Cisco UCS C220 M3 server.
3.2.1 Hardware and Software Installations of Cisco Content Server

- Hardware Installation of Cisco Content Server

We should connect power, USB keyboard, VGA Monitor and Ethernet (1 GB).

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power button/Power status LED</td>
</tr>
<tr>
<td>2</td>
<td>Identification button/LED</td>
</tr>
<tr>
<td>3</td>
<td>System status LED</td>
</tr>
<tr>
<td>4</td>
<td>Fan status LED</td>
</tr>
<tr>
<td>5</td>
<td>Temperature status LED</td>
</tr>
<tr>
<td>6</td>
<td>Power supply status LED</td>
</tr>
<tr>
<td>7</td>
<td>Network link activity LED</td>
</tr>
<tr>
<td>8</td>
<td>Asset tag (serial number)</td>
</tr>
<tr>
<td>9</td>
<td>KVM connector — Use this port for initial configuration</td>
</tr>
<tr>
<td>10</td>
<td>Hard drives (two), hot-swappable (2.5-inch drives installed in slots 1 and 2; slots 3 to 8 are empty)</td>
</tr>
</tbody>
</table>

*KVM = keyboard, video, and mouse*
Fig. 3.3 Content Server Rear Panel

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power supplies (two)</td>
</tr>
<tr>
<td>2</td>
<td>Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane)</td>
</tr>
<tr>
<td>3</td>
<td>Standard-profile PCIe slot on riser (full-height, half-length, x16 lane)</td>
</tr>
<tr>
<td>4</td>
<td>VGA video connector</td>
</tr>
<tr>
<td>5</td>
<td>Serial port (RJ-45 connector)— <strong>Not used</strong></td>
</tr>
<tr>
<td>6</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
</tbody>
</table>
| 7 | Dual 1-Gb Ethernet ports:  
LAN1 (Arrow 7, left pointer)— **Use this port to connect the Content Server to the network**  
LAN2 (Arrow 7, right pointer)— **Not used** |
| 8 | USB ports (two) |
| 9 | Identification button/LED |

- **Software Installation of Cisco Content Server**

Complete these tasks to install VM Content Server Release 6.1 on new hardware:

i. Install VMware vSphere ESXi

ii. Deploy OVA to Host

iii. Install Windows Server 2008 Standard R2 Service Pack 1

iv. Install Internet Information Services

v. Install Window Media Services

vi. Install Windows Server Features

vii. Install VM Content Server
3.2.2 Configuration of Cisco Content Server

After installations of hardware and software of the Cisco Content Server, we need to configure the Cisco content Server.

These are the detail initial configuration tasks as follows:

- Task 1: Connect and power on the Content Server and configure CIMC
- Task 2: Set the local administrator password
- Task 3: Enter the Windows Server 2008 activation key
- Task 4: Configure a static IP address
- Task 5: Set the date and time
- Task 6: Enable Remote Desktop Connection
- Task 7: Install a security certificate
- Task 8: Configure the H.323/SIP registration settings
- Task 9: Make a test recording

The test recording is a final task. You can try to make a test recording by dialing out and in. The detail work steps for recording by dialing out and in as follows:

Work steps for making a test recording by dialing out:

**Step 1** In the Content Server web interface, go to Management > Recordings > Create recording.

![Recordings in TCS Web Interface](image)

**Step 2** Select a recording alias.

**Step 3** For Dial number, enter the endpoint address that you want to call. Click Place call.
Step 4  Go to the **View Recordings** tab. You should see a thumbnail with a red recording dot for the recording in progress.

Step 5  End the call from the endpoint or by clicking on the thumbnail followed by **Edit recording** and **End call**.

Work steps for making a test recording by dialing in:

Step 1  In the Content Server web interface, go to **Management > Recording setup > Recording aliases**.

Step 2  Note the H.323 ID, E.164 alias, or SIP address (URI) for the Recording alias that you want to use.

Step 3  From an endpoint, dial one of the addresses that you noted.

Step 4  Go to the **View Recordings** tab. You should see a thumbnail with a red recording dot for the recording in progress.

Step 5  End the call from the endpoint or by clicking on the thumbnail followed by **Edit recording** and **End call**.

3.2.3  Using Cisco Telepresence Content Server

We can record and stream for Video (lecture) capture with Cisco Content Server. The Cisco TelePresence Content Server (Cisco TCS) is a network appliance that enables organizations to share knowledge and enhance communication by recording their video conferences and multimedia presentations for live and on-demand access.

The Cisco TCS can be scheduled by Cisco TMS to automatically include the Cisco TCS into any scheduled event or be used in the manner. The Cisco TCS workflow will automatically produce high quality videos of any standards based conference from a MCU, TelePresence Server, or directly from a TelePresence endpoint including the video participants and any secondary content such as a presentation.

We can use Cisco Telepresence Content Server to view recording, create and edit Recording, produce the resulting recordings in a range of formats and sizes to watch or download, and up loadings automatically to Media Experience Engine 3500, Show and share, Podcast Producer or iTunes U by Apple.

The Using Cisco Telepresence Content Server included as follows:

I.  The View Recordings
II. The My Recordings
III. Recordings Aliases
IV. Distribution Outputs
I. The View Recordings

From the View Recordings tab, we can watch a recording in the Content Server web interface, download an output of the recording for viewing on a device, or email a link to the recording to someone else.

- Watching a Recording in the Content Server Web Interface
- Watching a Downloaded Output on Your Computer
- Watching a Downloaded Recording on a Portable Device
- Sending a Link to the Recording to Others

- Work steps of watching a Recording in the Content Server Web Interface is the following:

To play the recording in a player in Content Server web interface

**Step 1** In a web browser, enter the URL of the Content Server.

**Step 2** If guest access is enabled, you see a list of recordings that guest users have permission to see. Guest users do not have to log in to play some or all of these recordings. If guest access is not enabled, you must log in (enter a username and password) to see a list of recordings.

**Step 3** Locate the recording that you want to view.

**Step 4** Click the thumbnail or the name of the recording.

**Step 5** Click the play button in the center of the recording.

By default, the Content Server displays the recording at the best quality for your connection, but you can also choose an internet speed. Under the recording, click the Set bandwidth preferences tab. Uncheck the automatically determine internet speed box. Then choose a speed from the Internet speed drop-down menu. If we choose a recording playback size that is too big for your internet speed, we might still be able to watch the recording, but it might occasionally stop playing and buffer.

- Work steps of watching a Downloaded Output on the Computer

**Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.

**Step 2** Under the recording, click the Download tab. If a recording does not have downloadable outputs, you will not see the Download tab.

**Step 3** Click the link for recording output that you want to download. A window for file download appears.

**Step 4** Click Save File, and put the recording where you want it on your computer.

**Step 5** You can double click the downloaded file for playback.

The recording is played back in the appropriate viewer for its format (in the program that is the default to play that type of media file on your computer). For example, if you have set up QuickTime to play .mp4 files and you download an MPEG-4 for Flash file, QuickTime plays the downloaded file.
• Work steps of watching a Downloaded Recording on a Portable Device

If a recording has downloadable outputs that are suitable for portable devices, we can download the recording and watch it on our iPod or Microsoft Zune device. We need to use a computer as an intermediary device and then load the recording on the portable device as we would any other file. After the recording has been loaded on the device, we can watch it as often as you like.

**Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.

**Step 2** Under the recording, click the **Share** tab.

**Step 3** Click **Email link**. The link appears in your default email application.

• Work steps of sending a Link to the Recording to Others

**Step 1** Locate the recording that you want to download. Click the thumbnail or the name of the recording.

**Step 2** Under the recording, click the **Share** tab.

**Step 3** Click **Email link**. The link appears in your default email application.

II. The My Recordings

The **My Recordings** tab is a list of recordings that you have created or recordings that others have given you permission to edit. The My Recording included two sections: Edit Recordings and Create Recording.

• Work steps of Edit Recordings are the following:

**Step 1** Click the **My Recordings** tab.

**Step 2** Click **Edit recordings**. A list of recordings that you created appears. This list also include recordings that others have given you permission to edit.

**Step 3** Locate the recording whose settings you want to edit.

**Step 4** Click **Edit recording**. A page that includes the settings for the recording appears.

**Step 5** Update recording settings as needed.

**Step 6** After updating the settings, click **Save**.

The Editing Recordings included Indexing a Recording, Cropping a Recording, Removing a Middle Section from a Recording and Joining Recordings. Users with the appropriate permissions and all site managers can manage recording outputs at any time.

• Work steps of Create Recording are the following:
There are two ways to create recording: Entering the number or address of the endpoint or system that the Content Server should call to make the recording, and Calling the Content Server from an endpoint or system. Call the Content Server with an H.323 ID, an E.164 alias, or a SIP address (URI).

Create Recording

We can create a recording by:

• Entering the number or address of the endpoint or system that the Content Server should call to make the recording.

• Calling the Content Server from an endpoint or system. Call the Content Server with an H.323 ID, an E.164 alias, or a SIP address (URI).

To create a recording by entering the number or address that the Content Server should call, do the following:

Step 1 In the web interface, log in to the Content Server as a creator.
Step 2 From the My Recordings tab, click Create recording.
Step 3 Select a recording alias from the Recording alias drop-down list.
Note For information about create recording parameters, see the Create Recording section.
Step 4 Enter the number or address of the endpoint or system that the Content Server should call to make the recording. You can configure the settings in the Recording information and Recording permissions sections before, during, or after recording.
Step 5 To join a password protected MCU conference, enter the PIN.
Step 6 Update Advanced call settings as needed.
Step 7 Click the Place call button when you are ready to start recording from the endpoint or system. If the recording alias that you use to record has the five-second countdown timer enabled, the countdown is displayed on the endpoint or system before recording starts. Recording starts when a red dot and ‘Recording’ is displayed on the endpoint or system.
Step 8 Click the End call button when you are ready to stop recording.
Step 9 Return to the web interface. Look for your recording in the View Recordings or My Recordings tab. From the My Recordings tab, you can Edit Recordings.

III. Recordings Aliases

To make recordings, creators must use a recording alias. A recording alias defines several properties, including ones related to dialing the Content Server from an endpoint for the recording session; specifying recording outputs; and indicating viewing and editing permissions.

There are two types of recording alias: System recording aliases, which can be used by any user in the creator or site manager role, and Personal recording aliases, which have owners in the creator role.
Owners can edit certain parts of their recording aliases: recording settings, default recording information, and default recording permissions.

Work steps for creating a new recording alias is the following:

To create a new recording alias, you must log in as a site manager.

Then in the Management tab, go to Recording setup > Recording aliases: Add recording alias.

IV. Distribution Outputs

We can configure the Content Server to upload recordings automatically to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U by Apple. The users with permissions can manually upload existing recordings to these products.

There are three ways to Distribution Outputs:

- Configuring Automatic Upload to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U.
- Uploading Existing Recordings to Cisco Media Experience Engine 3500, Cisco Show and Share Podcast Producer or iTunes U.
- Configuring Automatic Upload to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U.

To automatically upload recordings from the Content Server to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U, we must configure a media server configuration and a template:

Step 1  Create a media server configuration for the desired product. From the Management tab, go to Recording Setup > Media server configurations.

Step 2  Click one of the following: Add Media Experience Engine 3500 server configuration, Add Show and Share server configuration, Add Podcast Producer server configuration, or Add iTunes U server configuration.

Step 3  In the page that appears, configure settings to set up a relationship between the Content Server and the media server. See the “Media Server Configurations” section on page 1-46 for information about these settings.

Step 4  Create a template that has a distribution output that uses the server configuration that you created. From the Management tab, go to Recording Setup > Templates.

Step 5  Click Add template.

Step 6  In the page that appears, check Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U.
Step 7  In Outputs for distribution to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U section, check the Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes box. You can check the box only if Content Server has a media server configuration for Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U.

Step 8 From the Media server configuration drop-down menu, choose the desired media server configuration.

Step 9 Configure any other settings for the template. See the “Templates” section on page 1-39 for information about the other template settings.

Any recording that is created with a recording alias that uses the template that you made is automatically uploaded to the media server that is configured in that template.

After finishing the recording call, the Content Server transcodes the video recording files in the specified size. When transcoding is finished, the Content Server uploads the recording file to the media server with the credentials that were specified in the media server configuration.

If a user uses the Content Editor on the Content Server to edit the length of a recording that has an output that was already uploaded to the media server, the Content Server transcodes the recording and uploads the newly edited version to the external media server. Previous versions of the recording on that media server are not overwritten; the media server can have a number of recordings of different lengths that are from one Content Server recording.

- Uploading Existing Recordings to Cisco Media Experience Engine 3500, Cisco Show and Share, Podcast Producer or iTunes U.

Users with appropriate permissions can upload any existing recording to Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U:

Step 1 Locate the recording that you want to upload to an external media server. For that recording, click Manage outputs.

Step 2 In the page that appears, check Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U.

Step 3 In the Outputs for distribution to Distributed to Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U section, check the Media Experience Engine 3500, Show and Share, Podcast Producer, or iTunes U box. You can check the box only if Content Server has a media server configuration for Media Experience Engine 3500, Show and Share, Podcast Producer or iTunes U.

Step 4 From the Media server configuration drop-down menu, choose the desired media server configuration.

Step 5 For Show and Share or iTunes U, choose the recording size from the Size drop-down menu.

Step 6 Click Save.
After we click **Save** button, the Content Server transcodes the recording in the specified size. When transcoding is finished, the Content Server uploads the recording file to the media server with the credentials that were specified by the site manager in the media server configuration.

If a user uses the Content Editor on the Content Server to edit the length of a recording that has an output that was already uploaded to the media server, the Content Server transcodes the recording and uploads the newly edited version to the external media server. Previous versions of the recording on that media server are not overwritten; the media server can have a number of recordings of different lengths that are from one Content Server recording.

- **Distribution Outputs and Streaming Servers.**

From the **Management** tab, we can configure both media servers for distribution outputs and media servers for streaming by going to **Configure > Media server configurations**. We can configure relationship between the Content Server and one of the types of media servers in the network:

- Windows Media streaming server
- QuickTime or Darwin streaming server
- Wowza Media Server for Flash
- Media Experience Engine 3500
- Show and Share
- Podcast Producer
- iTunes U

The first four media servers stream recordings from those servers, but users view those recordings through the Content Server web interface. Streaming servers extend the scale and capabilities for streaming live and recorded calls; add the ability to live stream MPEG-4 for QuickTime and MPEG-4 for Flash; provide on-demand true streaming of MPEG-4 for QuickTime and MPEG-4 for Flash; and deliver live and on-demand media via the Adobe HTTP Dynamic Streaming protocol.

The last four media servers support distribution outputs, not streaming outputs.

4. Media Experience Engine for Lecture Video Capture Control

Media Experience Engine is a Lecture Video Capture Control to Transform and Share solution. Media Experience Engine included computer server for video files with database applications and Web Server for web broadcasting for show and share. We can build and develop the Media Experience Engine for Lecture Video Capture Control by Windows, Mac OS and Linux System. In fact many small and middle sizes companies, example Vyopta, Vimeo, Video.Show, globo.com have developed the Media Experience Engine Technology for Video Capture and show and share solution.
Cisco has provided Media Experience Engine: Cisco MXE 3500 for Lecture Video Capture Control. Cisco MXE 3500 is an enterprise video platform. The Capture, Transform, Share solution helps to enable video on demand, live streaming, and video speech search capabilities.

Cisco MXE 3500 delivers a powerful new way to find and view video content quickly and easily. Now we can allow viewers to search for specific content or speakers within individual videos with Pulse Video Analytics. It is easy video management for many users. Cisco MXE 3500 (Media Experience Engine) enables video everywhere in the enterprise.

With any to any media adaptation on the MXE 3500, recorded and live video content is automatically adapted from a range of incompatible media formats, resolutions, and speeds, from standard-definition [SD] up to full high-definition [HD], so they can be viewed on demand or live by a wide variety of playback devices and applications, such as Cisco Show and Share.

Cisco MXE 3500 has the media post-production capabilities. Support for live streaming formats including Windows Media and live MPEG-2 Transport Stream (MPEG-2 TS) so users can deliver live streams content to Cisco Digital Signs for communications, training, events or other applications.

Cisco MXE 3500 has been used in the Next Generation Classrooms for Transform in the San Jose State University.

![Fig. 4.1 Cisco MXE 3500 (Media Experience Engines)](image)

4.1 Installations of Cisco MXE 3500

This section provides an overview of the Cisco MXE 3500 V3 appliance external features. The Cisco MXE 3500 V3 appliance is based on the Cisco UCS C220 server.

- Hardware Installation of
1. **KVM** = keyboard, video, and mouse.

**Fig. 4.2 Cisco MXE 3500 V3 Appliance Front Panel Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Power button/Power status LED</td>
<td>Power supply status LED</td>
</tr>
<tr>
<td>2 Identification button/LED</td>
<td>Network link activity LED</td>
</tr>
<tr>
<td>3 System status LED</td>
<td>Asset tag (serial number)</td>
</tr>
<tr>
<td>4 Fan status LED</td>
<td>KVM¹ connector (used with KVM cable that provides two USB, one VGA, and one serial connector)</td>
</tr>
<tr>
<td>5 Temperature status LED</td>
<td>Hard drives (four), hot-swappable (2.5-inch drives installed in slots 1 to 4; slots 5 to 8 are empty)</td>
</tr>
</tbody>
</table>

¹ KVM: keyboard, video, and mouse.

---

**Fig. 4.2 Cisco MXE 3500 V3 Appliance Front Panel Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Power supplies (two)</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>2 Low-profile PCIe slot 2 on riser</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>(half-height, half-length, x8 lane)</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>7 Dual 1-Gb Ethernet ports:</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>LAN1 (Arrow 7, left pointer) — Use this port to connect the Content Server to the network</td>
<td></td>
</tr>
<tr>
<td>LAN2 (Arrow 7, right pointer) — Not used</td>
<td></td>
</tr>
<tr>
<td>3 Standard-profile PCIe slot on riser</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>(full-height, half-length, x16 lane)</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>4 VGA video connector</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>8 USB ports (two)</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
<tr>
<td>9 Identification button/LED</td>
<td>1-Gb Ethernet dedicated management port</td>
</tr>
</tbody>
</table>
We should connect power, USB keyboard, VGA Monitor and Ethernet (1 GB).

When we first set up the Cisco MXE 3500, perform the initial configuration described in this section to enter the IP address for the appliance and set the password for the administrator account. The initial configuration enables the Cisco MXE 3500 to connect to the LAN. We can then access the Cisco MXE 3500 Web UI and Windows desktop through its public IP address for additional configuration.

**Step 1** Connect the keyboard and monitor to the Cisco MXE 3500 rear panel.

**Step 2** Connect an Ethernet cable to the network port.

**Step 3** Power on the Cisco MXE 3500 standalone or Resource Manager (RM) appliance by using the front panel Power On/Off LED/Button.

**Step 4** Press Alt+F1 and then press Enter.

**Step 5** Log in with the following default credentials:
- Username: admin
- Password: change_it

The configuration wizard launches, and the Configure Network Settings screen appears. Fields marked with an asterisk (*) are required. The system highlights any input errors.

**Step 6** Enter the network settings for your deployment. Click Next.

**Step 7** Click OK at the Please Wait screen, and click OK at the Success screen. The Configure Hostname and Domain Name screen appears.
Step 8  (Optional) Enter a hostname and domain name. Click Next. The Configure DNS Server screen appears.

Step 9  (Optional) Enter a DNS Server IP address. Click Next. The Configure NTP Server screen appears.

Step 10 (Optional) Enter an NTP server. Click Next. The Modify and Synchronize Admin Password screen appears.

Step 11 Enter and re-enter a new password for the admin user account. Click Next. This updates and synchronizes the administrator account password for the Linux OS, Windows OS, and ESXi interfaces.

Step 12 Click OK at the Please Wait screen, and click OK at the Password Changed screen.

Step 13 (Optional) To enable or disable a shared folder password, click the check box. Click Next.

Step 14 Click OK at the Configuration Complete screen. You have completed initial configuration.
• Work steps of initial Server Setup

**Step 1** Attach a supplied power cord to each power supply in your server, and then attach the power cord to a grounded AC power outlet.

**Step 2** Connect a USB keyboard and VGA monitor by using the supplied KVM cable connected to the KVM connector on the front panel.

**Step 3** Open the Cisco IMC Configuration Utility:

- Press the **Power** button to boot the server. Watch for the prompt to press F8.
- During boot up, press **F8** when prompted to open the Cisco IMC Configuration Utility. Note the differences between versions of Cisco IMC firmware:
  
  – In Cisco IMC 2.0(1) and later, there are two windows for this utility that we can switch between by pressing F1 or F2 (see Figure 2-6 for sample windows). The IPv4 and IPv6 protocols and dynamic domain name system (DDNS) are supported. You can also define a host name and a DDNS domain.
  
  – In Cisco IMC earlier than release 2.0(1), there is only one window for this utility. Only the IPv4 protocol is supported. DDNS is not supported.

**Step 4** Set NIC mode and NIC redundancy.

**Step 5** Choose whether to enable DHCP for dynamic network settings, or to enter static network settings.

**Step 6** Optional: Use this utility to make VLAN settings.

**Step 7** Optional: Set a host name for the server.

---

*Fig. 4.7 Cisco IMC Configuration Utility Window 1 and Window 2 (Cisco IMC 2.0(1) and Later)*

**Step 8** Continue with the next action based on which release of Cisco IMC your server is running:

- Cisco IMC earlier than release 2.0(1)—Skip to Step 14.
- Cisco IMC 2.0(1) and later—Press **F1** to go to the second settings window, then continue with the next step. From the second window, you can press F2 to switch back to the first window.
Step 9 Optional: Enable dynamic DNS and set a dynamic DNS (DDNS) domain.
Step 10 Optional: If you select the Factory Default check box, the server will be set back to the factory defaults.
Step 11 Optional: Set a default user password.
Step 12 Optional: Enable auto-negotiation of port settings or set the port speed and duplex mode manually.
Step 13 Optional: Reset port profiles and the port name.
Step 14 Press F5 to refresh the settings you made. You might have to wait about 45 seconds until the new settings appear and the message, Network settings configured is displayed before you reboot the server in the next step.
Step 15 Press F10 to save your settings and reboot the server.
Step 16 Connect to the CIMC for server management. Connect Ethernet cables from your LAN to the server,
using the ports that you selected by your NIC Mode setting in Step 4. The Active-active and Active-passive NIC redundancy settings require you to connect to two ports.
Step 17 Use a browser and the IP address of the CIMC to connect to the CIMC Setup Utility. The IP address is based upon the settings that you made in Step 4 (either a static address or the address assigned by your DHCP server).

4.2 Configuration of Cisco MXE 3500 by using web interface

We can now access the web UI at http://mxe_IP_address/mxeui/ (where mxe_IP_address is the hostname or IP address for the Cisco MXE 3500 standalone or RM appliance) for configuration with the following default login credentials:

User Name—admin
Password—admin

4.2.1 Work Steps of Configuring the Host Settings

Now we can be working on Administration page after login User Web Interface.

Step 1 From the Toolbox, select Administration > Host
Step 2 Modify the Host:
   a. From the Host Administration menu, click the arrow to the right of Host Options > Edit. The Edit Host pop-up displays.
   b. In the Host Name field, enter the Host name. This name must be a valid computer name that you configured for the standalone Cisco MXE 3500.
   c. In the Temp Directory field, enter the local or UNC path for the temp folder on the Host that you configured in Step b.
   d. Click Save. The modified Host displays in the Hosts pane.

Step 3 Add workers to the Host that you created in Step 2. In the Workers tab, click Permit All.
All workers, except two, will go green.

Step 4 At the top of the page, click Apply Configuration.

Step 5 If you have a clustered deployment, create a new host for each RN in your cluster.
   a. From the Host Administration menu, click the arrow to the right of Host Options > New.
   b. In the New Host pop-up, enter the required information.
   c. Repeat steps 3 and 4.

4.2.2 Work steps of Configuring the Input and Output Media Directories

For the Cisco MXE 3500 to obtain input and store output media, we must configure the input and output directories. We should ensure that any directories that we are going to configure exist and are shared.

Step 1 Log into the web UI as an administrator.
Step 2 From the Toolbox, select Administration > System.
Step 3 In the following fields of the Input section, enter the directories where Cisco MXE 3500 will obtain input media, such as \mxe_IP_Address\media.
• Bumper
• Common
• Media
• Watermark

Step 4 In all the fields in the Output section, enter the directories where Cisco MXE 3500 will store output media, such as `\mxe_IP_Address\output`.

Step 5 Clicks Save.

4.2.3 Work steps of Configuring User Settings

Access the User Administration page from the Toolbox by clicking Administration > User to set user access and permissions.

The top pane of the User Administration page displays the predefined user. The lower pane displays the permissions for each user. The New or Edit Users pop-up allows you to create and modify system users. The user settings included User Name, Password, Confirm Password, First Name, Last name, E-mail and Role.

4.2.4 Configuring the Video Conversion Interface (SUI)

The Cisco MXE 3500 provides an easy to use Video Conversion Interface that is oriented for end users who want to convert between video formats while providing minimal details. End users access the Video Conversion Interface at `http://mxe_IP_address/sui`.

To use the interface, the user simply points to a video on a local drive, uploads it, and provides a title and description. The user can then request converted output in various file formats with the addition of bumpers, trailers, overlays, and watermarks. No choice of these assets is possible; all are preconfigured through the SUI Administration page.

1. Access the SUI administration page from the Toolbox by clicking Administration > SUI Admin.
II. General Settings Section

The General Setting Section included Maximum provisioned users, access code, user ID and so on. The detail information can be found in Fig. General Setting Section.

III. Media File Assets Settings

The Media File Assets Settings included Bumper, Trailer, Watermark Files, Graphic Overlay Template and Graphic Overlay content.
IV. Show and Share Settings

The Show and Share Settings included Enabled (checkbox), Authentication URL, Admin Userid, Admin Password, End Point, Upload URL and Automatically Approve Video (checkbox).

V. Stream Server Settings

There is only check box for Stream Server Settings.
4.2.5 Configuring Shared Folders

Secure the shared folders by configuring Active Directory (AD) mode or Local User Access mode. The Configuring Shared Folders included three sections as follows:

- Accessing the Shared Folder Access Settings
- Active Directory Mode
- Local User Access Mode

- Accessing the Shared Folder Access Settings

From the Toolbox, expand Administration, and click Shared Folder Access Settings. The Shared Folder Access page displays.

- Active Directory Mode

First, identify or create an account in the AD that is authorized to join the Cisco MXE 3500 to the AD domain. Secondly, you should configure the NTP (Network Time Protocol) server.

Enable Active Directory Mode

To enable AD, do the following in the Shared Folder Access Settings page:

Step 1 Check Secure.

Step 2 Check Enable Active Directory, and enter the required information in the input fields.

Step 3 Click Save.

Step 4 RDC to mxe_IP_address, where mxe_IP_address is the hostname or IP address for the Cisco MXE 3500, to access the Windows OS. Login as admin and enter the password created during initial configuration.

Step 5 At the Command Prompt, enter AddServiceUser username password. The username and password are the Service Account username and password entered in Step 2.
script creates the new user on the Windows platform. It then associates all MXE services to the new user.

**Step 6** Restart the Cisco MXE 3500 application:

a. SSH to *mxe_IP_address*. The login prompt appears.
b. Login as admin. The Cisco MXE Appliance Configuration Menu displays.
c. Select Restart Cisco MXE Application.
d. Click OK.

• Local User Access Mode

Use the local user access mode if your Enterprise does not have an AD or chooses not to tie the system with the AD. To enable local user access mode, do the following in the Shared Folder Access Settings page:

**Step 1** Check Secure.
**Step 2** Check Local User Access.
**Step 3** Enter password.
**Step 4** Click Save.

4.3 Using Cisco MXE 3500 Web User Interface

The Administrator and users will use Cisco MXE 3500 Web User Interface to configurations and administrations.

4.3.1 Accessing the Cisco MXE 3500 Web UI

Access the Cisco MXE 3500 web UI at http://*mxe_IP_address*/mxeui/, where mxe_IP_address is the hostname or IP address for the Cisco MXE 3500.

On the Log In prompt, enter User Name: admin. Enter the password created during initial configuration, or the changed password if you have changed the password from the Cisco MXE 3500 Web UI.

![Login Cisco MXE 3500 System](image)

**Fig. 4.14 Login Cisco MXE 3500 System**

4.3.2 Information Panel
This Information Panel provides the following information:

- **Server**: Displays the host name of the Cisco MXE 3500.
- **User**: Displays the name of the user currently logged into the Cisco MXE 3500.
- **Profile Space**: Displays the profile space.
- **Logout**: Select this link to log out of the Cisco MXE 3500 or log in as a different user.
- **Change Password**: Click this link to change the Cisco MXE 3500 web UI admin password. The Change Password dialog displays (Figure 1-4). This changes the Cisco MXE 3500 web UI admin password only.

![Fig. 4.15 User Interface Components in Cisco MXE 3500](image)

**4.3.3 Menu Bar**

The menu bar offers the following options:

- **File**: Create a New Profile, Open a Profile, Change Password, or Log Out.
- **View**: View offers the same options that are available from the Toolbox, page 1-8. Select **Customize** to display or hide user interface components (Navigation column, Toolbox, and Profile Browser).
- **Tools**: Reset License Cache: Reset licensing information within the UI application. This option is typically performed by an administrator when a Cisco MXE 3500 license is changed / updated on the ECS. Choosing the Reset License Cache operation updates the Cisco MXE 3500 UI with the latest license information.
• **Help**: View the software version number, contact Cisco MXE 3500 Technical Support, or read Help files.

4.3.4 Toolbox

The Toolbox is a navigation tool that allows you to quickly view any section:

• **Submission**: Used to submit File or Live jobs.
• **Profile Management**: Used to create and manage component profiles (Preprocessor, Encoder, Distribution) and Job Profiles.
• **Administration**: Used to manage host, system, user and role permissions, profile space, custom metadata, Video Conversion Interface (SUI), API, LDAP, and shared folder access settings.
• **Monitoring**: Used to monitor job status, timed job status, system status, and node health status.
• **Reports**: Used to create custom status reports.
• **Folder Attendant**: Used to set up watch folders and track automatically ingested jobs.

4.3.5 Profile Browser

Click Search (next to Filter Text) to populate the results, then click Create New Profile. This option is not present if you do not have the correct permissions for profile editing.

4.3.6 Main Window

The Main Window displays the page selected from the Toolbox or from the View menu.

5. Show and Share for Video Lecture Capture

The Video Show and Share is a webcasting and video sharing application that helps organizations create secure video communities with user-generated content. The Show and Share provides the ability to create live and on-demand video content and define who can watch specific content. The Show and Share is a secured social network for collaboration, communication, learning, and pleasure—unlimited by time and place. People use Show and Share to improve information, communities, themselves, and each other. As a Show and Share administrator, we set the system-wide preferences and settings, assign user roles, integrate other devices with Cisco Show and Share, manage content, and generate system-wide reports.

Cisco has provided hardware and software for video show and share. Cisco MXA UCS M3, UCS 210-M, UCS 200-M2, MCS 7835-H3, WAVE-574, DMM on MCS 7835-H3, and DMM on UCS C210 (DMM-SVR-C210-K9) have supported Video Show and Share and Digital Media Manager (DMM). Here we only listed the installations of Cisco MXA UCS M3 Server. The most of Initial Server Setting is same.

We can also integrate TelePresence Content Server (TCS) and MXE 3500 with Cisco Show and Share.
5.1 Installation for Cisco Show and Share and Digital Media Manager Release 5.3.10 on the Cisco MXA UCS M3 Server

- Hardware Installation of Cisco MXA UCS M3 Server

Fig. 5.1 Cisco MXA UCS M3 Server Front Panel Features

<table>
<thead>
<tr>
<th>1</th>
<th>Power button/Power status LED</th>
<th>6</th>
<th>Power supply status LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Identification button/LED</td>
<td>7</td>
<td>Network link activity LED</td>
</tr>
<tr>
<td>3</td>
<td>System status LED</td>
<td>8</td>
<td>Asset tag (serial number)</td>
</tr>
<tr>
<td>4</td>
<td>Fan status LED</td>
<td>9</td>
<td>KVM connector (used with KVM cable that provides two USB, one VGA, and one serial connector)</td>
</tr>
<tr>
<td>5</td>
<td>Temperature status LED</td>
<td>10</td>
<td>Drives, hot-swappable (four 2.5-inch drives installed in slots 1-4; slots 5-8 are empty)</td>
</tr>
</tbody>
</table>

Fig. 5.1 Cisco MXA UCS M3 Server Front Panel Features

<table>
<thead>
<tr>
<th>1</th>
<th>Power supplies (two)</th>
<th>6</th>
<th>1-Gb Ethernet dedicated management port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane)</td>
<td>7</td>
<td>Dual 1-Gb Ethernet ports (LAN1 and LAN2)</td>
</tr>
<tr>
<td>3</td>
<td>Standard-profile PCIe slot on riser</td>
<td>8</td>
<td>USB ports</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 VGA video connector</td>
<td>Rear Identification button/LED</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Serial port (RJ-45 connector)</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 5.2 Cisco MXA UCS M3 Server Rear Panel Features

- **Initial Server Setting up and Installing the Cisco MXA UCS M3**

We should connect power, monitor and keyboard to access Cisco IMC Configuration Utility. The Initial Server Setting up and complete installation instructions are same with Cisco UCS C220 Server Installations. The detail work step can be found in 4.1 Installations of Cisco MXE 3500 (UCS C220 Server).

5.2 Using Cisco Show and Share

- **Access Cisco Show and Share**

To access Cisco Show and Share, point your web browser to:

http://server_name

In the above URL, replace server_name with the name of Cisco Show and Share server, for example http://video.example.com. Do not use an IP address.

When Cisco Show and Share loads, you see a Show and Share homepage as follows

Fig. 5.3 Show and Share homepage

- **Sign In to Cisco Show and Share**
We must be signed-in to Cisco Show and Share to access the administrator functions. The administrator functions that we can access depend on the administrator role or roles. The administrator roles included Category Administrator, Reports Administrator, Administrator and superuser.

The work steps to sign-in to Cisco Show and Share as follows:

**Step 1** Click the **Sign In** link in the global navigation area at the top of the page.

**Step 2** When the login dialog appears, enter your username and password and click **Log In**. You are returned to the Videos page.

- Access the Administration Area

**Step 1** To access the administration area of Cisco Show and Share, click the **Show and Share** link in the global navigation area at the top of the page.

**Step 2** Click **Administration**.

The Cisco Show and Share administration area appears. What you see depends upon the administrator permissions that you have.

The administrator in the illustration below has all three administrator roles assigned, so all of the options are available. The Reports menu would not be visible if the administrator did not have the Reports Administrator role.

If the administrator only had the Reports Administrator role, they would see the following when they logged into the administration area:

- User Roles and Privileges
The user roles in Cisco Show and Share included Visitor, Video Author, Video Publisher, Live Event User, Category Administrator, Reports Administrator and Administrator.

The detail information about the user roles in Cisco Show and Share included Visitor is the following:

<table>
<thead>
<tr>
<th>Role</th>
<th>What the role can do:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor</td>
<td>Visitors can typically browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
<tr>
<td>Video Author</td>
<td>Video Authors upload, record, and edit videos. They can submit videos for publication. They can browse and view videos. They may also be able to comment on, rate, and tag videos. To record video in Cisco Show and Share, Video Authors must have a video upload permission attached to their user profile.</td>
</tr>
<tr>
<td>Video Publisher</td>
<td>Video Publishers approve videos for publication. They can browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
<tr>
<td>Live Event User</td>
<td>Live Event Users edit, publish, administer, and delete live events. They can browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
<tr>
<td>Category Administrator</td>
<td>Category Administrators create and delete categories. They can browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
<tr>
<td>Reports Administrator</td>
<td>Reports Administrators run and view Cisco Show and Share reports. They can browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Administrators assign permissions to other users and set site-wide preferences. They can reset your password if you forget yours. They can browse and view videos. They may also be able to comment on, rate, and tag videos.</td>
</tr>
</tbody>
</table>

- Show and Share Home

The Home page is the starting point of Cisco Show and Share experience. We can always navigate back to the Home page by clicking Videos in the menu bar.
At the top of the Home page are featured videos. Below the Featured Videos are the Public Videos. These are videos that do not have any viewing restrictions attached to them. By default, the newest videos are shown at the top of the list. You can also sort the list by the most watched, the highest rated, or containing the most comments. When sorted by the number of comments, both general comments and timeline comments count towards the comment total for a video.

Videos with viewing restrictions appear on the Private tab in your My Account page if you have permission to access them. For the “superuser” account, private videos also appear on the home page.

You can filter the public videos by selecting a tag, a category, entering a filter term, or any combination of those methods. You can also change the Public Videos list view.
Any time we click a video, the Video Playback page appears. When the page loads, the video begins to play automatically.

Fig. 5.8 Video Playback

1. Video title and detail information.
2. Video player.
3. Video information tabs. The Info tab appears for every video. Other tabs appear depending upon the features used by the video.
4. Comment area. General comments about the video are shown on the Commentary tab. Comments from the timeline are shown on the Timeline Comments tab.
5. Author information. You can send the author an e-mail message, subscribe to an RSS feed of the author’s videos, or see more videos from the author.
6. Videos related to the current video. The author can choose specific related videos or let the system pick the videos (based on them having tags and categories in

- My Account

Click My Account in the menu bar to access the My Account page. We must be logged-in to access this page.
Fig. 5.9 My account in Cisco Show and Share

1. Status Updates and Messages. Notifications about comments on your videos and publishing status appear in this area.

2. Add a Video. (Author or Live Event role required) You can start the upload or video record process from this page. You can also configure and schedule a live event.

3. Action Items and Requests. If you are a video approver (if your Show and Share has the Video Approval process enabled), your pending approvals appear in this area.

4. Videos. This area contains the videos you have uploaded, live events you have scheduled, and videos that have viewing restrictions (that you can view).

- Upload Video

Access the Upload Video page by clicking **Add Video > Upload** a Video on the Home page or by clicking **Upload Video** on the My Account page. We must be logged-in to access this page. If you are not logged-in, you will be prompted to do so.
Fig. 5.10 Upload in Cisco show and Share

1. Video Information. You can add a title, description, and tags to the video.
2. Add Video. Specify the video to upload.
3. Add Optional Files. You can upload slides to be synchronized with the video, a text transcript of the video, and downloadable files to accompany the video.

- Record a Video

Access the Upload Video page by clicking **Add Video > Record** a Video on the Home page or by clicking **Record Video** on the My Account page. You must be logged-in to access this page. If you are not logged-in, you will be prompted to do so.
Video Information. You can add a title, description, and tags to the video.

Capture Settings. Specify the audio and video capture devices and record your

Add Optional Files. You can upload slides to be synchronized with the video, a text transcript of the video, and downloadable files to accompany the video.

- Publish Your Video

The Video Summary will be showed for publish after Upload Video or Record Video.
1 Video Summary. Contains the video information you entered in the Upload Video or Record Video screen. You can edit this information before publishing.

2 Page Permissions. You can restrict access to the video, assign it to one or more categories, and disable the following features for the video you are publishing if the features have been enabled globally:

- Commenting on videos
- Commenting anonymously
- Rating videos
- Tagging videos
• Sharing videos

![Image of Video Sharing interface]

![Image of Scheduling interface]

Fig. 5.13 Add related and Scheduling in Publish

1. Add Related. You can manually specify related videos or have the system automatically select them based on tags and categories assigned to the videos.

2. Scheduling. You can schedule when you want the video to appear in Cisco Show and Share and when you want it removed from public viewing.

5.3 Using Cisco Digital Media Manager (DMM)

Cisco Digital Media Manager (DMM) included four sections: Show and Share, Administration (DMS-Admin), cast and Digital Signs.

Cisco Show and Share administration depends on services provided by Cisco Digital Media Manager (DMM). The software that provides these additional features and services is called Cisco DMS Administration (DMS-Admin). For example, although we assign user roles in the Cisco Show and Share administration screens, users are defined in DMS-Admin.

Because of these dependencies, your Cisco Digital Media Manager must always be reachable from Cisco Show and Share for Cisco Show and Share to function properly.

• Start Digital Media Manager (DMM)

**Step 1** Browser at DMM appliance: https://dmm.example.com:8443.

**Step 2** Login Digital Media Manager (DMM) by your account.
Step 3  Click Log In.

Step 4  Choose Administration from the global navigation or click Administration on the landing page.
• DMS-Admin Dashboard

The dashboard for DMS-Admin centralizes many features for system monitoring and log collection. When problems of any kind interfere with the data-collection processes that populate its gauges, they show question marks in addition to the best available data. In this case, check and confirm that the systems and network are configured and working correctly.

Fig. 5.16 Dashboard in Digital Media Manager

The Dashboard included Alerts Gauge, System Information Gauge, Status Gauge, Licensed Features Gauge, and Users Logged In Gauge.

• Check Processes Remotely

**Step 1** Start DMS-Admin.
**Step 2** Choose **Administration > Services**.
**Step 3** View the processes for Show and Share
Click Show and Share Server in the far-left column. A list tells you which processes are running or stopped.
Fig. 5.17 Processes for Show and Share

The Server Processes included Apache, OpenAM Web Application, Streaming Server, Tomcat, Postgresql, DMS-Admin Web Application and so on.

- Allow or Disallow Video Transcoding

**Step 1** Start DMS-Admin.
**Step 2** Choose **Settings > External Servers > MXE**. rK Steps of enable Show and Share Use of MXE Features:

![Settings](image)

**Step 3** Click **Enabled**.

![Enabled](image)

**Step 4** Enter the fully qualified (DNS-resolvable) domain name of your MXE appliance.

![General Settings](image)

**Step 5** Enter the ftp login credentials for your MXE appliance.
Step 6 Enter the MXE-relative directory paths where MXE should:

- Find incoming video files from Show and Share (“input”).
- Save its transcoded versions of these files (“output”).

Step 7 Click Save.

- Users and Groups

User roles in DMS-Admin are the automatic result of a logical operation. We cannot use DMS-Admin to assign a user role directly to any user. In some cases, the users who are authorized use more than one licensed feature of Cisco DMS. The DMS-Admin user role that you see for a user account is based on all privileges and access settings that the user has, combined across all of the licensed and activated features.

The user roles included Admin, Group Admin and ReadOnly.

Work Steps of create User Groups:

Step 1 Choose Administration > Users.
Step 2 Click Create Group.
Step 3 Enter values to name and describe the group.
Step 4 Click Save to save your work.

Work steps of create User Accounts

Step 1 Choose Administration > Users.
Step 2 Click Add New User.
Step 3 Enter the required values in the Add New User dialog box.

Step 4 (Optional) Enter contact information.
**Step 5 (Optional)** Assign the user to a user group.

**Step 6** Click *Save*

Work Step of Assign Users to Groups:

When you first create a user account in DMS-Admin, you can associate the account with a user group immediately or you can do so after you assign access rights and permissions to the user.

Drag a user from the table to the group name.

Use the Edit User dialog box.
Work steps of edit User Accounts:

You can edit user account settings manually.

**Step 1** Choose **Administration > Users**.
**Step 2** Click an entry in the untitled table that describes all user accounts.
**Step 3** Choose **Options > Edit User**.

![Fig. 5.27 Editing user](image1)

**Step 4** Make changes to its values in the Edit User dialog box.

![Fig. 5.28 Changing user information](image2)

**Step 5 (Optional)** Enter contact information.

![Fig. 5.29 Enter contact information.](image3)

**Step 6 (Optional)** Assign the user to a user group.
Step 7 Click Save

Assign User Access Rights and Permissions:

Assign access rights and privileges to users in the individually licensed features they will use.
5.4 Show and Share for Video Lecture Capture from Vyopta

Vyopta is Cisco Partner. Vyopta has developed the Show and Share for Video Lecture Capture program and software with Cisco TelePresence endpoint: C 90, content server and MXE 3500 in the Smart Classroom by vPublish. Vyopta vPublish provided video recording and upload video for Show and Share with graphic user interface. San Jose State University will develop and create 51 Next-Generation Learning smart classrooms with Cisco & Vyopta.

Fig. 5.33 Smart Classroom (Next Generation classroom) for Video Lecture Capture in San Jose State University

- Cisco TelePresence Video Equipment with Vyopta vPublish in Smart Classroom

Cisco TelePresence Video Equipment has been used for Video Lecture Capture in Smart Classroom. These TelePresence equipment included Cisco TelePrence Codec C90, Cisco TelePrence Content Server (TCS), and Media Experience Engine: Cisco Transform MXE 3500.

Cisco TelePrence Content Server (TCS) makes it easy for lecturers to record content from any H.323 or SIP Videoconference unit with a built-In web-based Interface.

The record lecture can then be transcoded and enhanced using Cisco Media Experience Engine, with the option to include graphical elements and even tags for easy navigation and consumption. The lecture can then be published using the Cisco Show and Share application, a webcasting and video-sharing
solution that enables simple archiving and retrieval of stored video assets, giving students the option to watch the content on desktops, mobile devices, or the Cisco TelePresence system.

Vyopta vPublish works smoothly in the background to automate the workflow for streamlined publication of content through Integration with SJSU's Student Information Services (SIS), which is built on Oracle PeopleSoft Enterprise Campus Solutions.

The vPublish solution establishes a single alias based on a data-driven workflow, reducing the IT burden of managing volumes of aliases. vPublish applies SIS metadata throughout the content process, automatically tagging content with relevant information and eliminating the need for manual lecturer input. The solution also creates defined security groups, automatically routing content to the right location for secure access by authorized users. The result is more comprehensive and more tightly controlled content that is easy to publish and find.

- Using Vyopta vControl and vPublish in Smart Classroom

There is a Vyopta vControl for vPublish to Presentation, Call, Meeting and Record in the Smart Classroom.

Fig. 5.34 vControl Screen

The information about operations of vControl with vPublish is the following:

I. Presentation,
II. Call,
III. Meeting
IV. Record

The video lecture capture can be recorded in the smart classroom.

The detail information about operations for Vyopta vControl can be found in our eCampus documents.

- Using Show and Share in the Smart Classroom

Cisco has provided Show and Share Technology in the Smart Classroom (Next Generation Classroom). The detail operation information can be found in 5.2 Cisco Show and Share:

The detail information about Access Cisco Show and Share

- Sign In to Cisco Show and Share
- Access the Administration Area
- User Roles and Privileges
- Show and Share Home
The technology of Lecture Video Capture allows professors and teachers to connect, present, record and share anytime and anywhere. The faculties can record and share their lectures online for the students to watch repeatedly.

The live web broadcasting and show and share of Lecture video capture have been applied to distance learning and eCampus. The students can study the courses anywhere on the world.

The design and development smart classroom for lecture video capture is very interesting and important project. We can begin to set up the smart classroom for lecture video classroom by cheaper camera, microphone, monitor, and computer server following the requirement of Endpoint, content server and media experience engine, and show and share. Of course we can use Cisco equipment directly for lecture video capture in the smart classroom. We believe the classical education system will be changed and reformed quickly by lecture video capture in the smart classroom and through with Internet development.