Administration

This chapter includes the following topics:

Introduction to Administration

This section includes the following topics:

Administration Section of the Toolbox

Note You must have Admin Tools permission to perform these tasks.

The Administration section of the Toolbox enables you to manage the following:

- Host Administration, page 14-2: Used to configure computers to be recognized by the Cisco MXE 3500. This includes defining and specifying the function of the Host and any workers configured for that Host.
- System Administration, page 14-13: Used to define directory locations and other system-wide settings.
- User Administration, page 14-23: Used to create and manage user access to the Cisco MXE 3500.
- Role Administration, page 14-28: Used to create and manage user roles in the Cisco MXE 3500.
- Profile Spaces, page 14-33: Used to manage multiple profile directories within the Cisco MXE 3500.
- User Metadata, page 14-36: Used to create custom name/value pairs that can be submitted with each job.
- IP Capture (Live Streaming), page 14-39: Used to create and manage IP Capture sources.
- Video Conversion Interface (SUI), page 14-43: Used to configure the Conversion Interface for end users.
- API Administration, page 14-48: Used to configure the authentication mode and password.
- LDAP Settings, page 14-49: Used to configure LDAP settings.
- Shared Folder Access Settings, page 14-52: Used to configure Active Directory settings.

Additional Administrative Tools

The following administrative tools are also provided with Cisco MXE 3500:

- Cisco MXE 3500 Tools, page 14-57
- Profile Converter, page 14-58
- Database Configuration, page 14-66
- Log Viewer, page 14-67

Host Administration

This section includes the following topics:

- Introduction to Host Administration, page 14-3
- Understanding Host Administration, page 14-4
- Creating a New Host, page 14-5
- Enabling/Disabling a Host, page 14-7
- Editing Host Settings, page 14-8
- Deleting a Host, page 14-8
- Adding Workers to a Host, page 14-9
- Removing Workers from a Host, page 14-10
- Configuring Node Attributes, page 14-11

Introduction to Host Administration

The Host Administration page allows administrators to configure the Cisco MXE 3500 to work with computers on the network. Host is simply another word for the computer or system that runs the Cisco MXE 3500. The Host Administration page is used to tell the Enterprise Control System (ECS) what the Hosts are capable of running (what the load capacity of the machine is and what software is installed).

Access the Host Administration page from the **Toolbox** by clicking **Administration > Host**.

Configure Network Settings

Each computer configured to work with the Cisco MXE 3500 must belong to the same domain or workgroup as the ECS. The exact network specifications will differ depending on the existing network and administrator preference. For domain installations, network configuration will include creating IUSR and the Cisco MXE 3500 domain user accounts. For workgroup installations, network configuration will include verifying that identical, valid IUSR and the Cisco MXE 3500 user accounts have been created on each local Host.

The Cisco MXE 3500 runs the services, and the IUSR account is used to give the Web server access to other network resources.

Configure and Activate Host

When the Host is created, click on the Host to load its configured workers in the lower pane of the UI. From this pane, enable and configure workers for that Host. Then click the **Apply Configuration** button. See also: Creating a New Host, page 14-5.

Understanding Host Administration

Select a Host to display summary information about workers configured on that Host. Table 14-1 describes the fields.

Table 14-1 Host Administration Fields and Descriptions

Field	Description
Host	This is the name of the machine running the Cisco MXE 3500 LCS (Local Control System) and workers. The computer name and the Host name must match exactly. To verify the computer name of a Windows Server computer, right-click the My Computer icon on either your desktop or in your Start Menu, select Properties, then select the Computer Name. For an NT computer, right-click Network Neighborhood, select Properties, and select the Identification tab. Alternately, type the hostname command at the command prompt to display the computer name.
Status	Displays the status of the Host: Enabled or Disabled. To change the status, right-click the Host or click Host Options, and select Enabled or Disabled. **Note**: If the status is disabled, jobs will not schedule on that Cisco MXE 3500 node.
Port	TCP (Transmission Control Protocol) port that the LCS is listening on (default is 3500).
Capacity	Reflects a numeric value (0-99) assigned for the total available processing capacity of the displayed Host. Capacity can be any number for a given Host, but it is important that all Hosts be numbered according to the same standards. For example, for one particular Host it will not matter if the total capacity is set at 5 or at 10. However, if there is another Host that has twice the capacity, the capacity of both Hosts should be listed in common terms. So, a Host that is twice as powerful would have a capacity of 10 if the first Host was 5, or 20 if the first Host was 10. Capacity is directly related to processor capacity, but may also be affected by drive speed, network congestion, and other factors. All of the factors that affect the amount of work a particular Host can do efficiently should be considered when assigning a capacity value. **Note** Numbers between 5 and 30 are typically best. Setting this to a high number > 30 can make the system status monitor hard to read. See also: Understanding Capacity, Limit, and Expense, page 14-10.
Temp Directory (UNC Name)	Specifies the directory where temporary files and preprocessor output will be stored. This must be entered as a UNC name so that other Hosts will be able to access files written to this directory. This is where preprocessor output and other temporary files will be written while the job is processing. Unless the Preprocessor box in the Output Profile is checked to specify that Preprocessor files should be saved, files written to the Temp Directory will be deleted automatically when encoding is complete.

Table 14-1 Host Administration Fields and Descriptions (continued)

Field	Description
Permitted?	A green checkmark indicates that the worker listed to the right is configured to run on the displayed Host and that it is currently online and available to process tasks. A red X indicates either: • That the worker listed to the right is configured to run on the displayed Host but is currently offline and cannot be contacted by the ECS, or, • The worker is not enabled or configured.
Worker	Displays a list of all workers that have been configured to run on the displayed Host. The Name, DV, DVCAM, Video Channel, and Audio Channel fields appear only for Live capture workers and define the location of the capture card on the Host. Channels are numbered sequentially from 0.
Licensed	Indicates the number of concurrent instances of this worker type (example: prefilter, encoder, distribution) that can be running on the system (all nodes controlled by that ECS). This value is defined in the Cisco MXE 3500 license file.
Limit	See the "Understanding Capacity, Limit, and Expense" section on page 14-10.
Expense	See the "Understanding Capacity, Limit, and Expense" section on page 14-10.
Capture Name	Defines the name associated with a live capture worker. Because Hosts can have more than a single video capture card and can be configured to run more than one Live capture worker, the Capture Name is required in order to identify the specific capture card used by the worker. This is only displayed for Live capture workers.
Capture Type	Type of capture card (DV, DVCAM, AJA-SDI, Custom, etc.). Selection of a non-custom value will predefine the audio and video channel
Video CH / Audio CH	Displays Video Channel and Audio Channel for each Live-capture worker.

Creating a New Host

When creating a Host, administrators must use the Windows Computer Account name (NetBIOS name) in order to create a Host that will be recognizable to the ECS.

See also: Creating a New Host Using the Right-Click Copy Option, page 14-7.

Procedure

Step 1 From the **Toolbox**, click **Administration** > **Host**.

Step 2 From the Host Administration menu, click the arrow to the right of **Host Options** > **New.** See Figure 14-1.

Figure 14-1 Creating a New Host

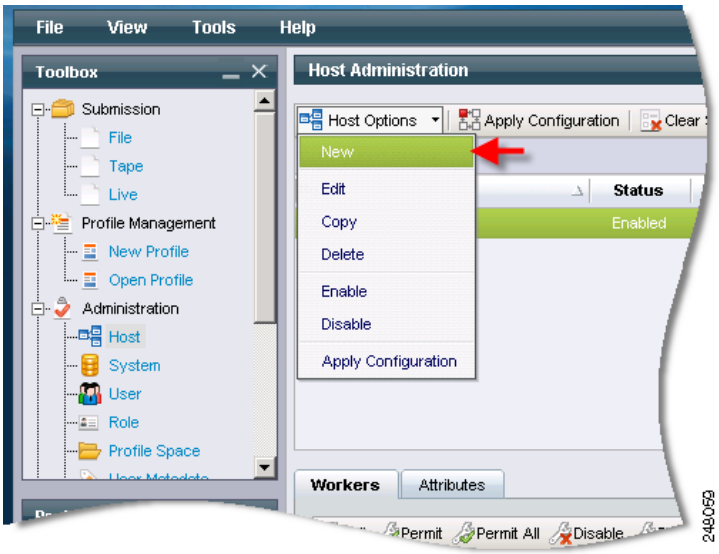
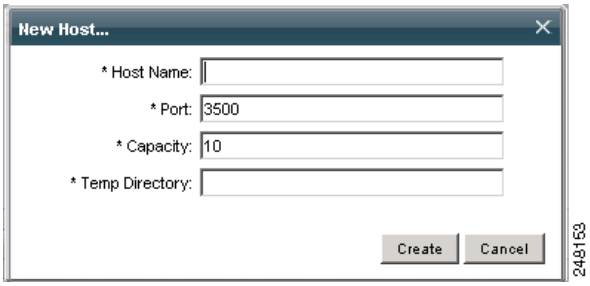


Figure 14-2 shows the pop-up that displays:

Figure 14-2 New Host Pop-up



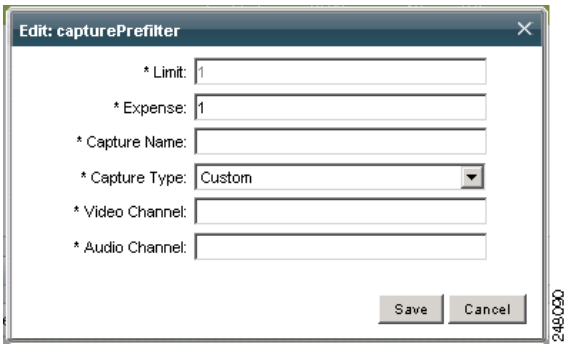
Step 3 Enter the required information (see Table 14-1), and click **Create**. The new Host displays in the Cisco MXE 3500 Hosts pane.

Step 4 Select each **Worker** that is assigned to the Host, and click **Permit**, or click Permit All.

Note If you select the Permit All option, only all non-Live workers will be permitted. Live workers require manual entry of additional data.

Step 5 Click each **Worker**, and click **Edit**. Figure 14-3 shows the pop-up that displays.

Figure 14-3 Edit Worker



Step 6 Enter the **Limit** and the **Expense**, and click **Save**. See also: Understanding Capacity, Limit, and Expense, page 14-10.

Step 7 For Live captures, enter Capture Name, Capture Type, Video CH, and Audio CH.

Step 8 At the top of the page, click **Apply Configuration**.

Note Workers added to a Host must be configured before tasks can be assigned to that worker. See also: Adding Workers to a Host, page 14-9.

Creating a New Host Using the Right-Click Copy Option

Follow the same steps as noted above, but select a Host, and click **Copy**. This creates a new Host with the same worker configuration, except that the Capturepreffilter worker settings are not copied to the new Host.

Enabling/Disabling a Host

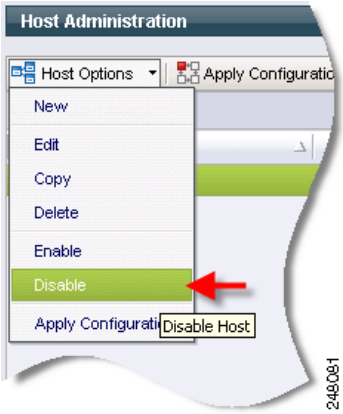
After a Host is created, click on the Host to load its configured workers in the lower pane of the User Interface. From this pane, enable and configure workers for that Host. Then, click the **Apply Configuration** button. See also: Creating a New Host, page 14-5.

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **Host** to display the Host Administration page.

Step 2 Highlight a Host, and click **Host Options** or right-click on the Host, and select **Enable** or **Disable**. See Figure 14-4.

Figure 14-4 Disabling a Host

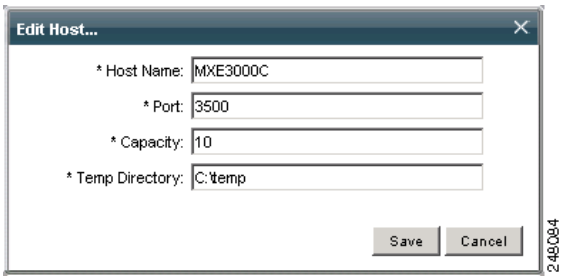


Editing Host Settings

Procedure

Step 1 From the **Host Administration** page, double-click the Host or click **Host Options**, and select **Edit**. Figure 14-5 shows the pop-up that displays.

Figure 14-5 Edit Host Pop-up



Step 2 Make any changes to the fields, and click **Save**.

Deleting a Host

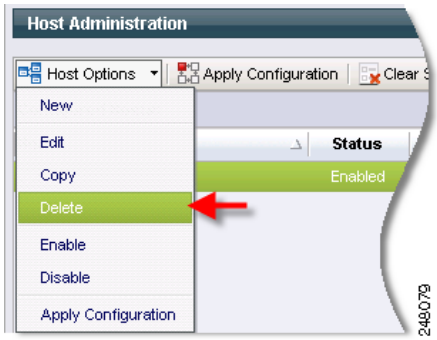
Procedure

Step 1 From the **Host Administration** page, select the Host to be deleted.

Step 2 Right-click the Host or click **Host Options** > **Delete**. See Figure 14-6.

Step 3 When the deletion confirmation pop-up displays, click **OK**.

Figure 14-6 Deleting a Host



Adding Workers to a Host

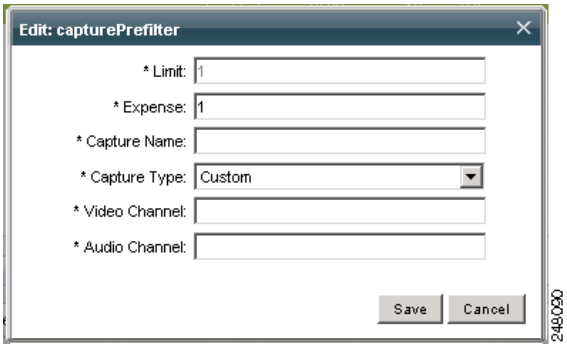
Procedure

Step 1 From the **Host Administration** page, select a Host.

Step 2 In the lower pane, select a **Worker**, and click **Permit**, or click Permit All. The list of workers displayed is controlled by your license level.

Step 3 Click a **Worker**, and click **Edit**. Figure 14-7 shows the pop-up that displays.

Figure 14-7 Edit Pop-up



Step 4 Enter the **Limit** and the **Expense**, and click **Save**.

Note The remaining four fields apply to Live captures.

Step 5 At the top of the page, click **Apply Configuration**.

Table 14-2 Worker Fields and Descriptions

Field	Description
Limit	Displays the maximum number of workers that can be run simultaneously on the displayed Host (0-99). Limits can only be modified on the Host page by Resource Manager level licensees. See also: Understanding Capacity, Limit, and Expense, page 14-10.
Expense	**Note**: Expense will be different for different types of workers. For example, MPEG encoding is more labor-intensive than Microsoft encoding. So, an MPEG worker is given a higher expense than a Microsoft worker. Expense can only be modified on the Host page by Resource Manager level licensees. See also: Understanding Capacity, Limit, and Expense, page 14-10.

Understanding Capacity, Limit, and Expense

The ECS uses capacity and expense to assign tasks to specific workers on specific Hosts in order to keep jobs moving through the encoding process in the most efficient way possible. The ECS uses Capacity and Expense to ensure that no single Host is over-burdened in order to prevent bottlenecks.

The processing power required by a particular type of worker may not always be the same. Limit is used with Capacity and Expense to accommodate this. For example, running one of a particular worker takes a certain amount, and running two may require double that amount. However, when a certain number is exceeded, the efficiency may degrade: Everything is fine until the fourth instance of the same worker is triggered. After this, the Host bogs down and performance suffers. Setting the Limit for this particular worker to three will prevent the ECS from triggering the fourth worker, even if there is sufficient capacity to accommodate the normal expense of the fourth instance. Because the expense would dramatically increase if the fourth worker were triggered, setting the Limit to three creates a threshold for the normal expense of a worker. Limit allows the administrator to set an upper limit on the number of instances that can run at the same time.

Removing Workers from a Host

Procedure

Step 1 From the **Host Administration** page, select a Host.

Step 2 In the lower pane, select a **Worker**, and click **Disable**, or click Disable All.

Step 3 When the disable confirmation pop-up displays, click **OK**.

Configuring Node Attributes

This section includes the following topics:

Node Attributes Overview

Node Attributes allow you to schedule specific job tasks or all tasks within a job against a set of Cisco MXE 3500 nodes that support those tasks.

Note Nodes commonly refer to Cisco MXE 3500 Resource Nodes that are part of a multi-MXE cluster.

The node attribute feature has two purposes:

1. To allow specific task license features that can only be scheduled against a particular set of nodes to be constrained to those nodes. A system node attribute is available to force preprocessor tasks to be scheduled against nodes that have been assigned this node attribute.
2. To allow a user to designate specific nodes for specific tasks or jobs. For example, a user may want to designate specific nodes for high priority jobs or a user may want to require that a given organization use a specific set of nodes. You can submit a job with user-defined metadata (UDM) that specifies the organization, matching the node attribute that has been previously defined for that organization.

Tasks Matching Multiple Node Attributes

If a task (or job) matches multiple Node Attributes it will only be scheduled on a node that supports all matching attributes.

Scheduling Errors

If a task requires a specific Node Attribute that has not been assigned to any node, the task and job will fail with the following message:

```
[ECS_MISSINGNODEATTRIBUTE] A task (type: microsoft, id: 175) requested non-existent node
attribute. [EC_COMPLETED] Task Execution 175 is now complete. Reason = Failed.
```

Configuration Examples

Table 14-3 shows examples of how to configure the XPath and Apply To Job parameters of a Node Attribute to target specific nodes.

Table 14-3 Configuration Examples

Name	Description	XPath	Apply to Job
Schedule all jobs with a priority of 1 on a given set of nodes	Priority 1 Jobs	/job[priority=1]	true

Table 14-3 Configuration Examples (continued)

Name	Description	XPath	Apply to Job
Schedule all Microsoft (Windows Media) encoding tasks on a given set of nodes	Microsoft Tasks	type[contains(., 'microsoft')]	false
Schedule all jobs from organization ID = 54 (specified via UDM) on a given set of nodes	Organization 54	/job/user-data-job/metadata/udm-item[@name='organizationid' and @value='54']	true

Assigning Node Attributes to a Host

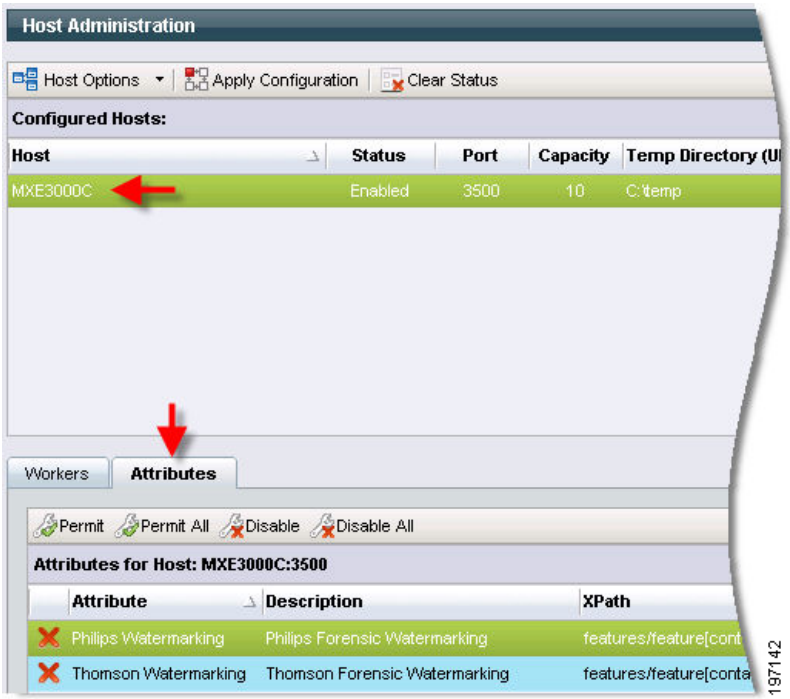
The Attributes tab of the Host Administration page is used to assign one or more Node Attributes to a specific Host (node). Once a Node Attribute has been created, it is listed on the Attributes tab. It is then permitted (assigned) or disabled.

Procedure

Step 1 In the upper **Host Administration** pane, highlight a **Host**.

Step 2 In the lower pane, click the **Attributes** tab, and highlight a **Node Attribute**. See Figure 14-8.

Figure 14-8 Assigning Node Attribute to a Host



Step 3 Click the **Permit** button.

Step 4 When the pop-up displays, click **OK**. The Node Attribute is now assigned or permitted.

System Administration

This section includes the following topics:

Introduction to System Administration

System Administration is used to define locations and parameters for files and directories used with the Cisco MXE 3500. It also includes settings for other system-wide parameters.

Access this page from the **Toolbox** by clicking **Administration > System**.

The System Administration page contains the following sections:

Input (System Administration)

Figure 14-9 shows Input settings. Table 14-4 describes the settings.

Figure 14-9 Input Settings

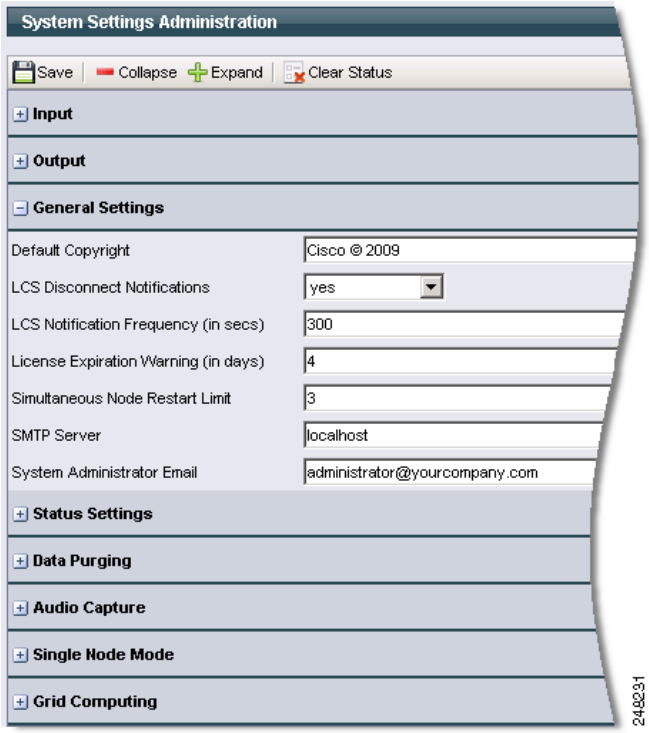


Table 14-4 Input Settings and Descriptions

Setting	Description
Bumper/Trailer Directory	Defines the location of files that can be used as bumpers or trailers to clips encoded with the Cisco MXE 3500. The Bumper/Trailer Directory controls the directory path where the Cisco MXE 3500 searches for files displayed in the Bumper Source and Trailer Source fields in the Preprocessing Profile page. The Bumper/Trailer Directory value can be entered either as a UNC path to a network share or to a mapped drive in the case of a deployment using a storage area network (SAN) or a single node deployment. The Bumper/Trailer Directory location must be accessible to all hosts.
Common Directories	Defines the directories where media files will be stored. Multiple directories can be defined. A semi-colon is used to separate directory entries. The Common Directory values can be entered either as a UNC path to a network share or to a mapped drive in the case of a deployment using a storage area network (SAN) or a single node deployment. The Common Directory locations must be accessible to all hosts.

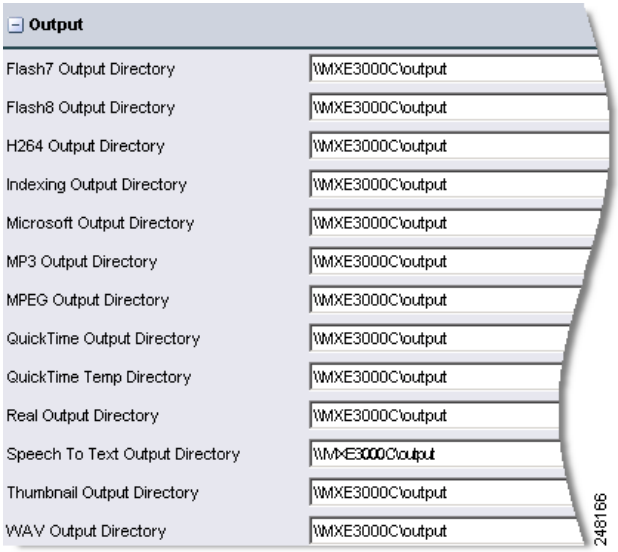
Table 14-4 Input Settings and Descriptions (continued)

Setting	Description
Media Directory	Defines the directory where media files that will be submitted to the Cisco MXE 3500 are stored. The Media Directory controls the directory path where the Cisco MXE 3500 searches for files displayed in the Source box on the File Submission page. The Media Directory value can be entered either as a UNC path to a network share or to a mapped drive in the case of a deployment using a storage area network (SAN) or a single node deployment. The Media Directory location must be shared and accessible to all Hosts. The System Administration page will give a warning if the value entered is not a UNC path, which is recommended. If using a mapped drive, all nodes configured to work with the Cisco MXE 3500 must have the location mapped as the same drive.
Profile Directory	Defines the default path the ECS will use to search for profiles when processing a submitted job.
Valid Input Extensions	Defines the list of valid extensions for files in Common Directories. Only files with extensions listed in this field will be displayed in the Selection List window in the Input section of the File Job Submission form. A semi-colon is used to separate file-extension entries.
Watermark Directory	Defines the location of files that can be used as watermarks for clips encoded with the Cisco MXE 3500. The Watermark controls the directory path where the Cisco MXE 3500 searches for files displayed in the Source drop-down in the Watermark section of the Preprocessing Profile page. The Watermark Directory value can be entered either as a UNC path to a network share or to a mapped drive in the case of a deployment using a storage area network (SAN) or a single node deployment. The Watermark Directory location must be accessible to all hosts.

Output (System Administration)

Figure 14-10 shows Output settings.

Figure 14-10 Output Settings



Output Directories

Output Directories define the location the Cisco MXE 3500 will use to save files of each encoding format supported by the licensing levels of your Cisco MXE 3500 system. Encoded files will be saved to the defined directories when either no Distribution > Output Profile is included in the Job Profile or when the checkbox in the Save Local File section of the Output Profile has been checked.

The Microsoft Output Directory value can be entered either as a UNC path to a network share or to a mapped drive in the case of a deployment using a storage area network (SAN) or a single node deployment.

General Settings (System Administration)

Figure 14-11 shows General settings. Table 14-5 describes the settings.

Figure 14-11 General Settings

Table 14-5 General Settings and Descriptions

Setting	Description
Default Copyright	Defines the default copyright information populated to the copyright field in all job submission pages. The Default Copyright is a system-wide setting. The value entered can be overwritten by the user when jobs are submitted by typing over the default information displayed.
LCS Disconnect Notifications	If yes, the Cisco MXE 3500 generates an e-mail (sent to the System Administrator) when an LCS disconnects from the ECS.
LCS Notification Frequency (in secs)	Frequency in seconds in which an LCS disconnect e-mail will be generated if multiple disconnects occur.
License Expiration Warning (in days)	Defines the period, in days, ahead of the license expiration date that an e-mail will be sent to the e-mail address defined in the System Administrator Email field.
Restart IP Capture/Webcast on Failure	yes: restart IP Capture on failure no: do not restart IP Capture on failure
SMTP Server	Identifies the e-mail server used to send e-mail notification messages. The server identified must be running the Simple Mail Transport Protocol (SMTP) service for it to process e-mail messages.
System Administrator Email	Stores an e-mail address used to contact the System Administrator. This e-mail address can be used to send messages to a regular e-mail account or to a text-enabled pager or cellular phone. The System Administrator e-mail address is used by Notification Profiles when the System Administrator options for From Email Address or To Email Address are selected.

Status Settings (System Administration)

Figure 14-12 shows Status settings. Table 14-6 describes the settings.

Figure 14-12 Status Settings

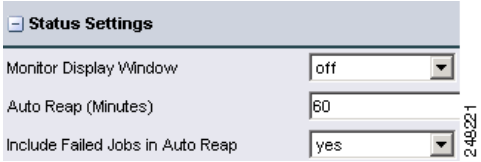


Table 14-6 Status Settings and Descriptions

Setting	Description
Monitor Display Window	This setting only applies in Console mode. If set to on, some workers (like preprocessor and encoders) will display a monitor window which displays the video being processed. **Note** This option does use system resources (example: cpu cycles, memory) and will slow down overall job processing. It may be used for debugging purposes or viewing encoded output.
Auto Reap (Minutes)	Defines the Auto Reap interval used to clear job information from monitoring pages. The time defined for Auto Reap determines how long information on a job will be displayed in monitoring pages before it expires. The Auto Reap interval is counted from the time the job completes.

Data Purging (System Administration)

Over time, Job data (job, task, executioncontext, executioncontextlog, and related tables) grow and fill up disk space. The Data Purging section allows you to configure automated system purging, physically deleting the appropriate records.

Note After initial or reset of Data Purging values, restart the CAM service to enable this feature or for changes to take place immediately.

Figure 14-13 shows Data Purging settings. Table 14-7 describes the settings.

Figure 14-13 Data Purging Settings

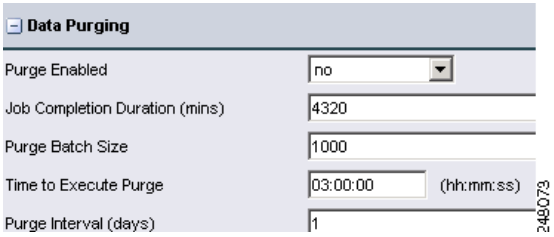


Table 14-7 Data Purging Settings and Descriptions

Setting	Description
Purge Enabled	**yes**: purge enabled **no**: purge not enabled
Job Completion Duration (mins)	In minutes, how long after the job was completed, before it is deleted.
Maximum Records to Delete	This setting limits the number of jobs to be deleted.
Time to Execute Purge	Configures the time of day the purge occurs.
Purge Interval (days)	Configures the number of days between purges.

Audio Capture (System Administration)

Figure 14-14 shows Audio Capture settings. Table 14-8 describes the settings.

Figure 14-14 Audio Capture Settings

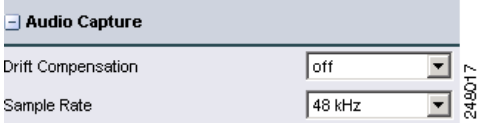


Table 14-8 Audio Capture Settings and Descriptions

Setting	Description
Sample Rate	Sets audio sampling rate to tradeoff audio quality and transmission bandwidth and file size limitations.

Single Node Mode (System Administration)

Figure 14-15 show Single Node Mode settings.

Figure 14-15 Single Node Mode Settings

Single Node Mode Settings

For users in bandwidth-sensitive environments, such as educational institutions and corporations, Single Node Mode provides greater control and the ability to confine encoding for a job to a single node.

Enabled: Enabling Single Node Mode forces all processing of a job to a single encoder node. The preprocessing, encoding, and distribution all takes place on one node rather then distributing the tasks across the system. This effectively reduces the amount of network traffic between the system nodes.

Disabled: Disabling Single Node Mode causes the system to distribute tasks to all the available nodes within a system. So, the preprocessing can occur on one node, the encode on another, and distribution on another. The Disabled setting allows more of the load balancing capabilities of the system. However, because the files are being moved through the workflow over multiple nodes, there will be more network traffic between the nodes within the system.

Soft node values Timeout/Queue Length have no range limit. The values need to be positive integers. The defaults are 3600 seconds (timeout) and 25 (queue limit).

The Timeout can be as large as you want. The value should be set relative to the average or maximum job length. You may want the tasks to flow to another node if the wait is going to be longer than the processing time and nodes are available.

Jobs are composed of Tasks. Tasks are the actual processes (preprocessing, encoding, and distribution) that together, make up a Job.

The Queue Length is set to a value that allows tasks to move to nodes that have a smaller queue. This value should be set relative to the average peak queue length the customer experiences. If the value is less than what normally occurs, performance will decrease.

These values are set to prevent individual nodes from getting backed up with Tasks. Single Node Mode can greatly improve performance for customers that do not have a network file storage system or do not have the network capacity to handle uncompressed AVI files. But, if individual nodes get backed up with more work, then performance is increased by letting the Tasks move to available nodes.

For customers with jobs/content that vary greatly in length or processing time, the system does not evaluate the input file or profile settings when distributing the tasks. For example:

20 jobs are submitted to a four-node system. Each fourth job is a full content encode that is 2 hours in length and will take an hour to process. The first three are a bumper, trailer, and preview encode that will be 15 to 30 seconds in length and take 5 – 15 seconds to run. If all are submitted sequentially in less than 5 seconds, the nodes will receive this distribution:

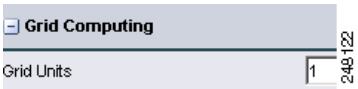
- Node 1: 4 bumper jobs - < 2 min total
- Node 2: 4 trailer jobs < 2 min total
- Node 3: 4 preview jobs < 2 min total
- Node 4: 4 content jobs > 4 hours total

In this case, the user would want the 3 jobs that are pending on node 4 to flow to the 3 empty (2 minutes after submission) nodes. Setting the timeout to 5-30 minutes would save 2 1/2 - 3 hours of processing time in this case.

Grid Computing (System Administration)

Figure 14-16 shows Grid Computing settings. **Grid Nodes**: Enter the number of nodes that will be included in the grid. See also: Flash Grid, page 8-16.

Figure 14-16 Grid Computing Settings



Setting Default Copyright Information

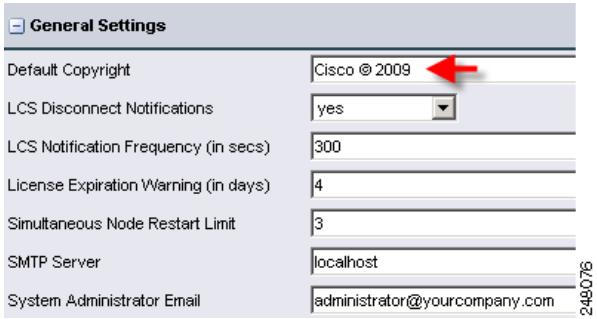
This setting defines the default copyright information populated to the copyright field in all job submission pages. The Default Copyright is a system-wide setting. The value entered can be overwritten by the user when jobs are submitted by typing over the default information displayed.

Procedure

Step 1 From the **Toolbox**, click **Administration > System**.

Step 2 In the **General Settings** section, enter the information in the **Default Copyright** field. See Figure 14-17.

Figure 14-17 Default Copyright Field



Step 3 Click **Save**.

Configuring Output File Storage Location

Note The LCS must have the appropriate user security level to create directories and write and delete files in the network directories defined on the System Administration page. See also: System Administration, page 14-13.

Procedure

Step 1 From the **Toolbox**, click **Administration > System**.

Step 2 In the **Input** and **Output** sections, in the appropriate field(s):

- For a **Network Directory**: Type in the UNC path to the directory where the corresponding files are stored.
- For a **SAN**: Type in the drive letter of the SAN and the directory path where the corresponding files are stored.

Step 3 Click **Save**.

Enabling Sys Admin E-mail Notification

Procedure

Step 1 From the **Toolbox**, click **Administration > System**.

Step 2 In the **General Settings** section, in the **System Administrator Email** field, enter the e-mail address.

Step 3 Click **Save**.

Step 4 Create a Notification Profile, page 9-12.

Step 5 Add the Profile to the Job. See also: Adding a Notification Profile to a Job Profile, page 9-16.

Turning Monitor Display Windows On/Off

This setting only applies in Console mode. If set to on, some workers (like preprocessor and encoders) will display a monitor window which displays the video being processed.

Note This option does use system resources (example: cpu cycles, memory) and will slow down overall job processing. It may be used for debugging purposes or viewing encoded output.

Procedure

Step 1 From the **Toolbox**, click **Administration > System**.

Step 2 In the **Status Settings** section, from the **Monitor Window Display** drop-down, select **on** or **off**.

Step 3 Click **Save**.

Setting the Auto Reap Interval for Job Monitoring

The Auto Reap interval is used to clear job information from monitoring pages. The time defined for the Auto Reap determines how long information on a job will be displayed in monitoring pages before it expires. The Auto Reap interval is counted from the time the job completes.

Procedure

Step 1 From the **Toolbox**, click **Administration > System**.

Step 2 In the **Status Settings** section, in the **Auto Reap (Minutes)** field, enter the desired number.

Step 3 Click **Save**.

User Administration

Activation To use this feature, you must purchase and install the Resource Manager feature license on the Resource Manager device.

This section includes the following topics:

Introduction to User Administration

The User Administration page is used by administrators to set user access and permissions.

Access this page from the **Toolbox** by clicking **Administration > User**.

The top pane of User Administration displays users that have been created. The lower pane displays the permissions for each user.

The Cisco MXE 3500 comes with one predefined user:

- **admin**: The predefined password is also **admin**. The password is changed during initial configuration.

Note Upon receipt of your system, the predefined admin user is the only user who can perform Folder Attendant administrative tasks such as creating users, assigning roles, deleting users, and denying or removing user permissions. **Do not delete the predefined admin user until you have created at least one new admin user**.

Creating New Users

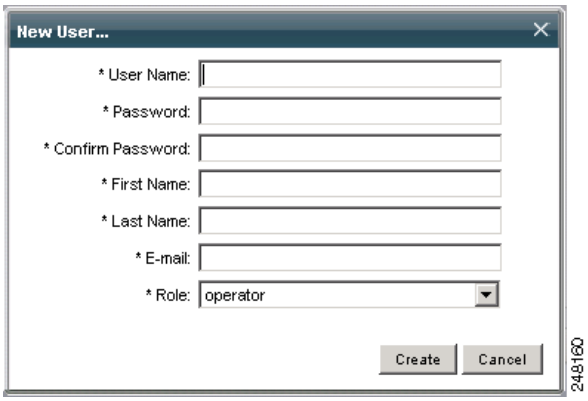
Each person using the Cisco MXE 3500 needs a user profile that controls their system access.

Procedure

Step 1 From the **Toolbox**, click **Administration > User**.

Step 2 From the menu bar, click **New**. The New Cisco MXE 3500 User pop-up displays. See Figure 14-18.

Figure 14-18 New User Pop-Up



Step 3 Enter the appropriate information in each of the fields as described in Table 14-9. All fields are required.

Table 14-9 New User Fields

Setting	Description
User Name	Enter a name for the new user.
Password	Enter a password for the new user.
Confirm Password	Re-enter the password to confirm it.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
E-mail	Enter the e-mail address of the user.
Role	Select the Cisco MXE 3500 role from the drop-down menu. The role defines the level of access the user has to Folder Attendant functions. Roles are defined at the time of deployment and are normally: Administrator and User.

Step 4 Select **Create** to save the new user.

Step 5 Select **Continue**. The new user displays on the User Administration page. The users are sorted in alphabetical order.

Updating Existing Users

Procedure

Step 1 From the **Toolbox**, click **Administration > User**.

Step 2 Select the user, and click Edit. See Figure 14-19. The Edit User pop-up displays, as shown in Figure 14-20.

Figure 14-19 Select the User to be Edited

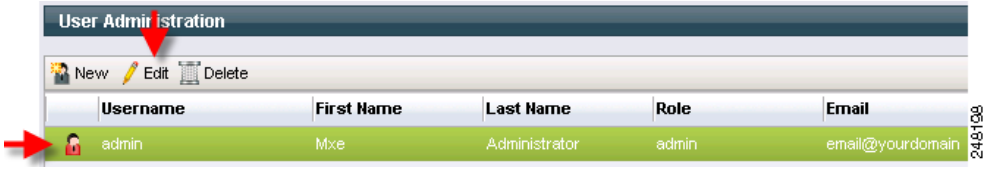
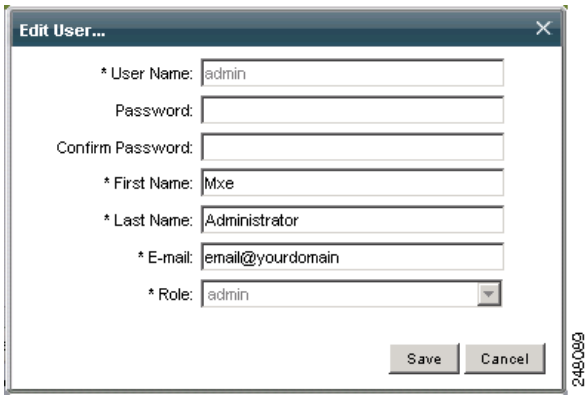


Figure 14-20 Edit User Pop-Up



Step 3 Update the information in any fields, as needed. The fields marked with an asterisk (*) are required. See also: Table 14-9.

Step 4 Click **Save**. The new information is saved and the User Administration page is updated.

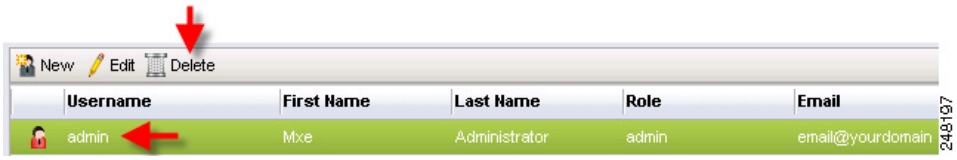
Deleting Users

Procedure

Step 1 From the **Toolbox**, click **Administration > User**.

Step 2 Select the user you want to delete, and click **Delete**. See Figure 14-21. A confirmation message displays, asking if you are sure you want to delete the selected user.

Figure 14-21 Select User to be Deleted



Step 3 Select **OK** to continue with the deletion.

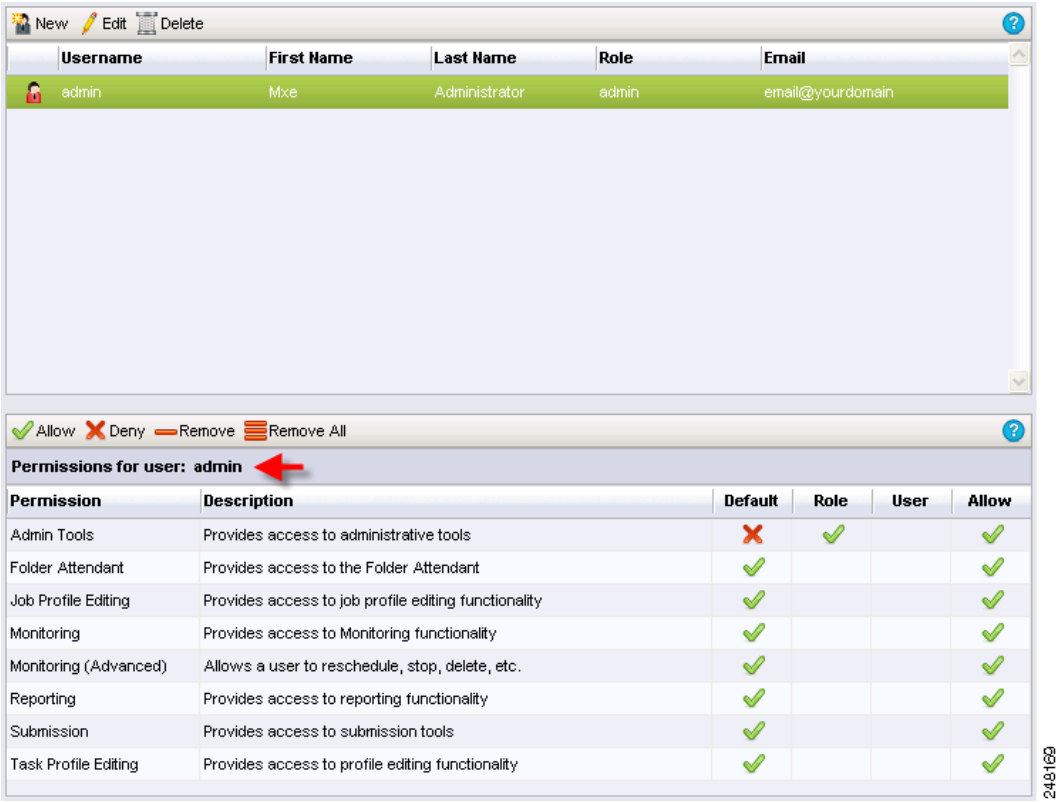
Setting User Permissions

After creating a user, the System Administrator sets permissions for that user. Each user is allowed or denied permission to use the following Cisco MXE 3500 features:

- **Admin Tools**: Provides access to Cisco MXE 3500 administrative tools
- **Folder Attendant**: Provides access to Folder Attendant
- **Job Profile Editing**: Provides access to Job Profile editing functionality
- **Monitoring**: Provides access to Monitoring functionality
- **Monitoring (Advanced)**: Allows a user to reschedule, stop, delete, etc.
- **Reporting**: Provides access to reporting functionality
- **Submission**: Provides access to submission tools
- **Task Profile Editing**: Provides access to profile editing functionality

The permissions for a selected user are displayed at the bottom of the page. See Figure 14-22.

Figure 14-22 Permissions for the Selected User



Four columns display the permissions that have been set for this user. Table 14-10 describes the settings.

Table 14-10 Columns in the Permissions Table

Column Name	Description
Default	Shows the default value for the permissions that are shipped with the Cisco MXE 3500.
Role	Shows the permissions set for the Role. Permissions set for the role override the Default permissions. The Role permissions specified in this column are set from the Role Administration page.
User	Shows the permissions set for the selected user. Permission set for the user override the Role permissions.
Allow	The actual permissions set for the selected user.

The red X indicates that permissions for that feature are denied, and the green check mark indicates that the selected user has permissions to access the feature.

Read the permission table from left to right: marks in the column to the right override the previous column.

The Default permissions are shown in the first column. These are default permissions that come loaded in the system.

The Role column shows the permissions for the Role assigned to this user. The permissions for the Role override the default permissions and are set on the Role Administration page.

The User permissions show the permissions for this specific user. These permissions override both the Default and Role permissions for this user only. Modify the permissions for the selected user shown in this column by following the procedure described below.

To quickly determine if certain permissions are allowed for a user, view the Allow column.

The picture above is an example of permissions set for the user named JSmith who has been assigned the user role. Notice that by default, those in the user role do not have access to Admin Tools (in this case) but have access to the remaining features. However, an administrator has added (overridden) the Admin Tools permission to this user's role.

For each feature, you can specify whether or not to allow, deny, or remove the user's access. You can also choose to remove all access to all features for a specific user.

Procedure

Step 1 From the **Toolbox**, click **Administration > User**.

Step 2 Select the user for which you want to set permissions from the top of the User Administration page. The permissions for the selected user are listed at the bottom of the page.

Step 3 Select the type of permission you want to modify. Your choices are:

- Admin Tools
- Folder Attendant
- Job Profile Editing
- Monitoring
- Monitoring (Advanced)
- Reporting
- Submission

- Task Profile Editing

Step 4 Click one of the buttons described in Table 14-11.

Table 14-11 User Permissions and Descriptions

Button Name	Description
Allow	Allow the user access to the specific feature.
Deny	Deny the user access to the specific feature.
Remove	Remove the user access to the specific feature.
Remove All	Removes all access to all features for the specific user.

Step 5 Repeat Step Step 3 to Step Step 4 for each feature to set all permissions for this user.

Role Administration

Activation To use this feature, you must purchase and install the Resource Manager feature license on the Resource Manager device.

This section includes the following topics:

Introduction to Role Administration

Each Cisco MXE 3500 user is assigned a role that controls their level of access to the various system features.

Access this page from the **Toolbox** by clicking **Administration > Role**.

The top pane of the Role Administration page displays roles that have been created. The lower pane displays the permissions for each role.

The Cisco MXE 3500 comes with three predefined roles:

- **admin**: Set up with permission to access all features.
- **operator**: Set up with permission to access Job Profile editing. Do not have access to admin tools and task profile editing features.
- **user**: Set up with permission to access all features, except administrative.
- **noaccess**: Assigned to Video Conversion Interface users. Do not have access to any adminstrative features.

Creating Roles

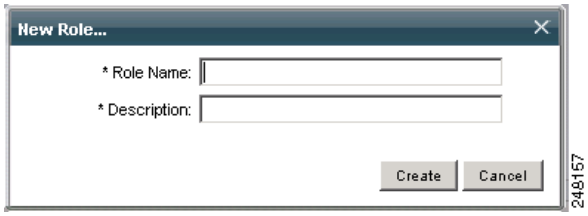
Use this procedure to create a new role.

Procedure

Step 1 From the **Toolbox**, click **Administration > Role**.

Step 2 From the menu bar, select **New**. The Create a New Role pop-up displays. See Figure 14-23.

Figure 14-23 New Role Pop-up



Step 3 Enter a **Role Name** and **Description**, and click **Create**. The new role displays on the Role Administration page. The roles are sorted in alphabetical order.

Updating Roles

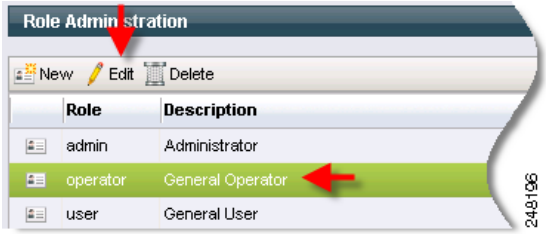
Use this procedure to update an existing role.

Procedure

Step 1 From the **Toolbox**, click **Administration > Role**.

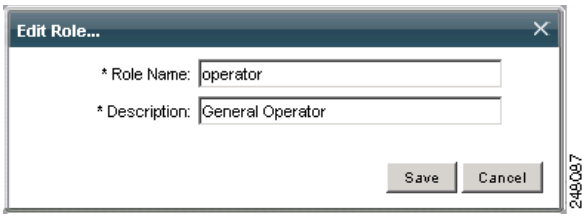
Step 2 Select the role you want to edit. See Figure 14-24.

Figure 14-24 Select Role to Edit



Step 3 Select **Edit** from the menu bar. The Edit Role pop-up displays. See Figure 14-25.

Figure 14-25 Edit Role Pop-up



Step 4 Update the information in each of the fields, as required. The fields marked with an asterisk (*) are required.

Step 5 When you are done updating the role, **Save** the new information. The updated information replaces the original information for the selected role.

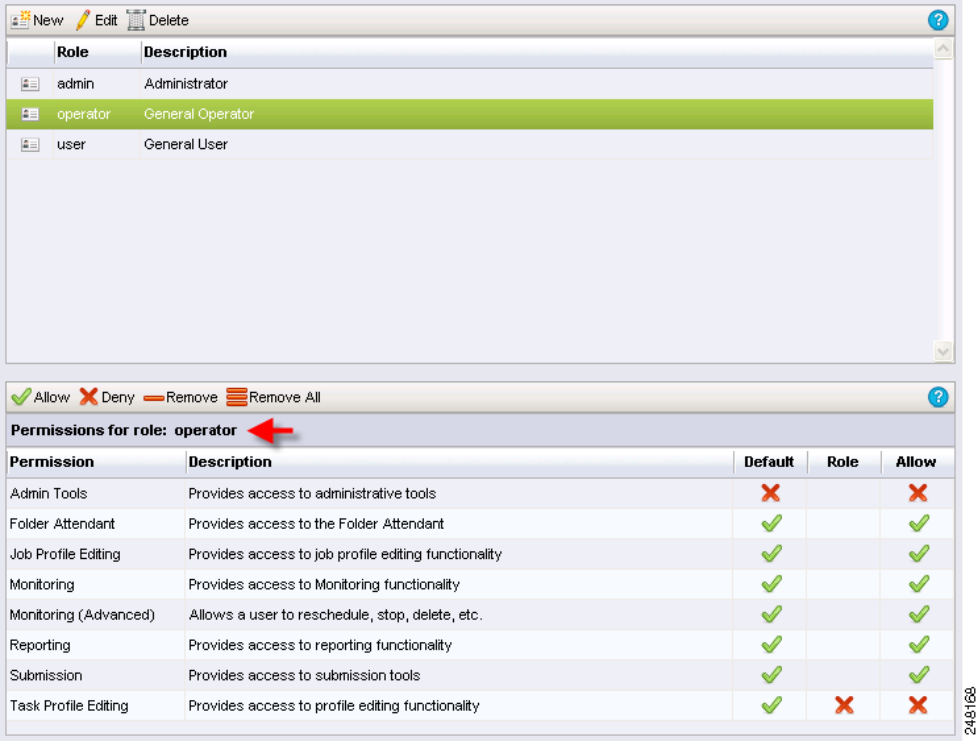
Setting Role Permissions

After creating a role, the System Administrator sets permissions for that role. Each role is allowed or denied permission to use the following Cisco MXE 3500 features:

- **Admin Tools**: Provides access to the Cisco MXE 3500 administrative tools
- **Folder Attendant**: Provides access to Folder Attendant
- **Job Profile Editing**: Provides access to Job Profile editing functionality
- **Monitoring**: Provides access to Monitoring functionality
- **Monitoring (Advanced)**: Allows a user to reschedule, stop, delete, etc.
- **Reporting**: Provides access to reporting functionality
- **Submission**: Provides access to submission tools
- **Task Profile Editing**: Provides access to profile editing functionality

The permissions for a selected role are displayed at the bottom of the page. See Figure 14-26.

Figure 14-26 Permissions for the Selected Role



Three columns display the permissions that have been set for each role. Table 14-12 describes the permissions.

Table 14-12 Selected Permissions

Column Name	Description
Default	Shows the default permissions that are shipped with Folder Attendant.
Role	Shows the permissions set for the Role. Permissions set for the role override the Default permissions.
Allow	The actual permissions set for the selected role, often the same as the Role column.

The red X indicates that permission for that feature are denied, and the green check mark indicates that the user in this role has permission to access the feature.

Read the permission table from left to right: marks in the column to the right override the previous column.

In the example above, the monitor role came loaded (by default) with access to Folder Attendant, Monitoring, and Submission features. In this case, an administrator has removed, for the role called monitor, access to Folder Attendant and Submission features. The monitor role now allows access to Monitoring functions only.

Modify the permissions for the selected role by following the procedure below.

For each feature, you can specify whether or not to allow, deny, or remove access. You can also choose to remove all access to all features for a specific role.

Procedure

Step 1 From the **Toolbox**, click **Administration > Role**.

Step 2 Select the role for which you want to set user permissions. The permissions for the selected user are listed at the bottom of the page.

Step 3 Select the permission you want to modify. You choices are:

- Admin Tools
- Folder Attendant
- Job Profile Editing
- Monitoring
- Monitoring (Advanced)
- Reporting
- Submission
- Task Profile Editing

Step 4 Select one of the buttons described in Table 14-13.

Table 14-13 Actions Related to Setting Permissions

Button Name	Description
Allow	Allow users in this role access to the specific feature.
Deny	Deny users in this role access to the specific feature.
Remove	Remove users in this role access to the specific feature.
Remove All	Removes all access to all features for the specific role.

Step 5 Repeat Step 3 and Step 4 for each feature to set all permissions for this role.

Deleting Roles

You can only delete a role if it contains no users. If the role contains users and you try to delete it, the following message displays:

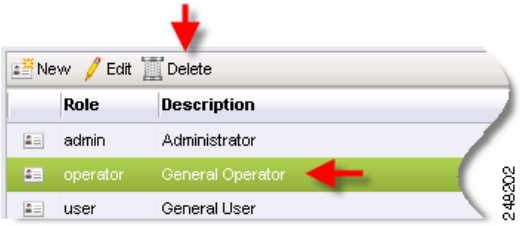
"The current role contains users and cannot be deleted."

Procedure

Step 1 From the **Toolbox**, click **Administration > Role**.

Step 2 Select the role you want to delete. See Figure 14-27.

Figure 14-27 Select the Role to be Deleted



Step 3 Click **Delete**. A confirmation message displays.

Step 4 Select **OK** to continue with the deletion. If the selected role does not contain users, it is removed from the list of roles on the Role Administration page.

Profile Spaces

Activation To use this feature, you must purchase and install the Resource Manager feature license on the Resource Manager device.

The Profile Spaces feature allows you to manage multiple profile directories within the system. The Cisco MXE 3500 is shipped with a single profile directory. The initial database setting for profiledir is:

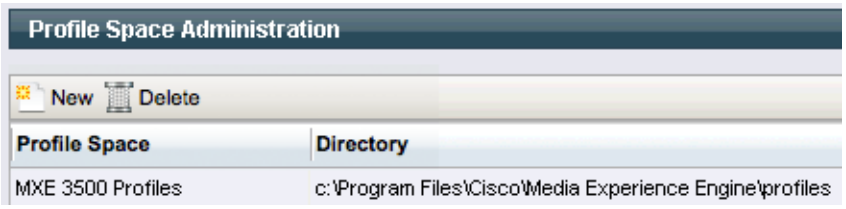
C:\Program Files\Cisco\Media Experience Engine\profiles

The Cisco MXE 3500 uses the system setting-configured profile directory to access the list of Job Profiles. However, you may want to maintain separate profile directories for separate groups or for separate customers.

You can create as many Profile Spaces as you need, but the Cisco MXE 3500 will check to see that each profile directory exists at the time of creation.

Your Cisco MXE 3500 session links to one Profile Space at a time, thereby determining the profiles that you can view from the Profile Browser. You can change your working Profile Space at any time by clicking **Tools** > **Select Profile Space**. See Figure 14-28.

Figure 14-28 Profile Space Administration



This section includes the following topics:

- Determining Your Current Profile Space, page 14-34
- Setting Your Current Profile Space, page 14-34
- Creating a Profile Space, page 14-35

- Editing a Profile Space, page 14-36
- Deleting a Profile Space, page 14-36

Determining Your Current Profile Space

Your current Profile Space is displayed in the upper right corner of the Web browser. See Figure 14-29.

Figure 14-29 Current Profile Space

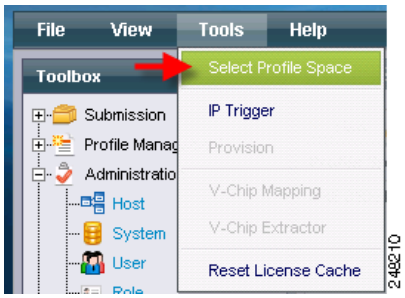
Setting Your Current Profile Space

Your Cisco MXE 3500 session links to one Profile Space at a time, thereby determining the profiles that you can view from the Profile Browser. You can change your working Profile Space at any time.

Procedure

Step 1 Click **Tools** > **Select Profile Space**. See Figure 14-30.

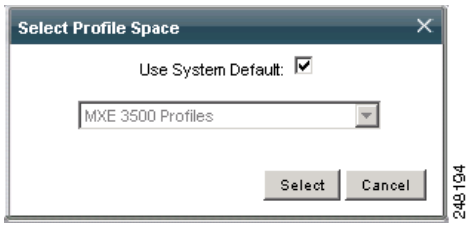
Figure 14-30 Selecting Profile Space



Step 2 A pop-up displays. See Figure 14-31. Select a Profile Space from the drop-down, and click the **Select** button. The browser is now reset to the selected Profile Space.

Note If no Profile Spaces appear in the drop-down, see the "Creating a Profile Space" section on page 14-35.

Figure 14-31 Selecting a Profile Space



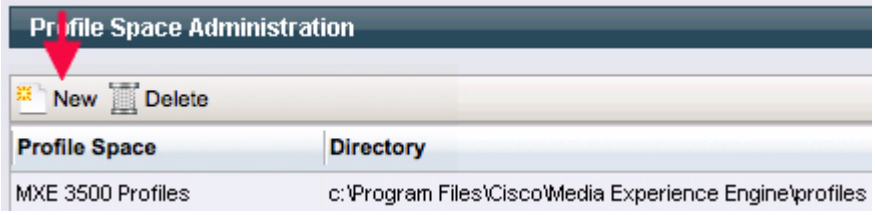
Creating a Profile Space

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **Profile Space**.

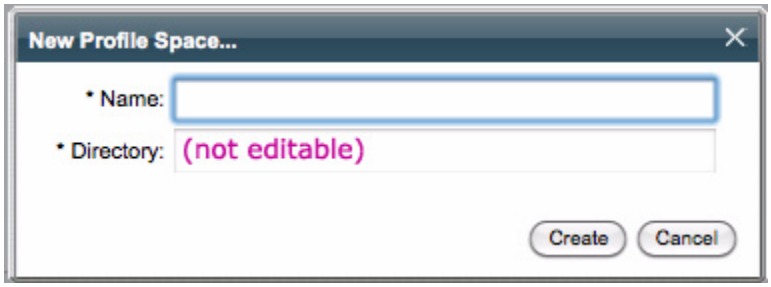
Step 2 In the Profile Space Administration pane, click **New**. See Figure 14-32. A pop-up displays.

Figure 14-32 Creating New Profile Space



Step 3 Enter a unique **Name** and click **Create**. See Figure 14-33. The new Profile Space displays in the Profile Space Administration pane. Profile spaces are always created in c:\mxe\profile\spaces\[profile space name]. The path to the profile space is fixed.

Figure 14-33 Entering Name and Directory



Editing a Profile Space

The editing of Profile Spaces is disallowed in Release 3.1 and later.

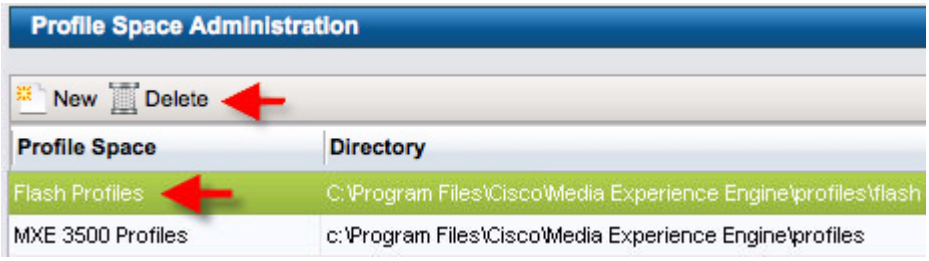
Deleting a Profile Space

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **Profile Space**.

Step 2 In the **Profile Space Administration** pane, select the **Profile Space**, and click **Delete**. See Figure 14-34.

Figure 14-34 Selecting a Profile Space to Delete



Step 3 When the deletion verification pop-up displays, click **OK**. The Profile Space is removed from the Profile Space Administration list.

User Metadata

Activation To use this feature, you must purchase and install the Resource Manager feature license on the Resource Manager device.

This section allows you to create custom name/value pairs that can be submitted with each job (and each task in the job). This custom metadata is returned in detailed job status including the HTTP POST job-status XML. This metadata (if submitted) is also stored in the database for each job and can be used for reporting purposes (like tracking which organization submitted which jobs) or (via HTTP POST) where it is passed back to other systems (like Velocity).

The Data Type can be defined as Integer, String, Decimal, or Enum (Enumeration). This type is used for validation when entering the user metadata values on the Job Submission pages.

Access this page from the **Toolbox** by clicking **Administration > User Metadata**.

This section includes the following topics:

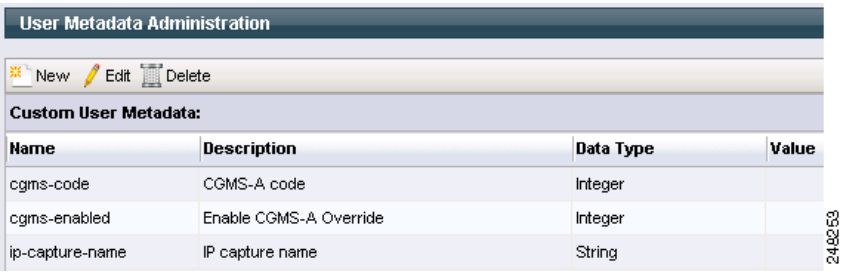
Adding User Metadata

Use this procedure to add a custom name/value pair.

Procedure

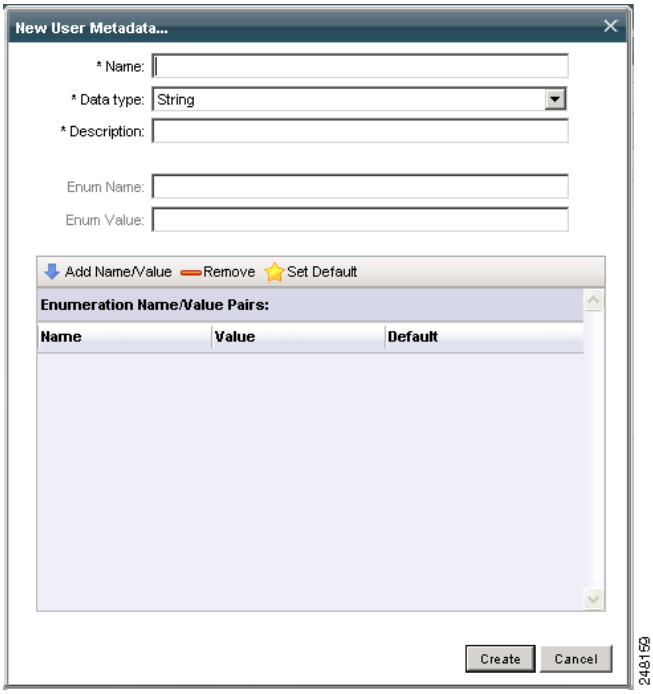
Step 1 From the **Toolbox**, expand **Administration**, and click **User Metadata** to display the page shown in Figure 14-35.

Figure 14-35 User Metadata Administration Page



Step 2 Click **New** to display the pop-up shown in Figure 14-36.

Figure 14-36 New User Metadata Pop-up



Step 3 Complete the fields, and click **Create**. The new name/value pair appears on the User Metadata Administration page.

Editing User Metadata

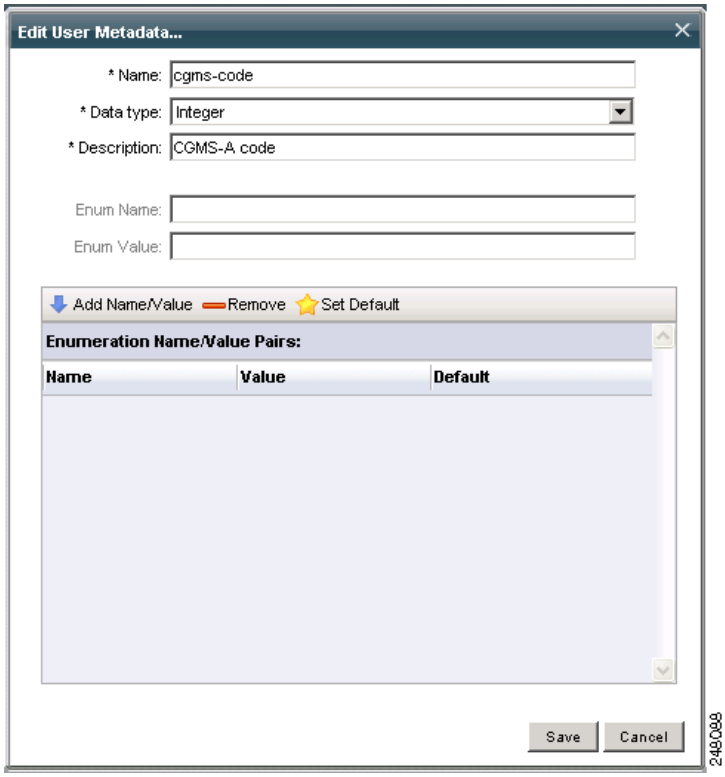
Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **User Metadata** to display the page shown in Figure 14-37.

Figure 14-37 Selecting User Metadata to Edit

Step 2 Highlight a metadata row, and click **Edit** to display the pop-up shown in Figure 14-38.

Figure 14-38 Edit User Metadata Pop-up



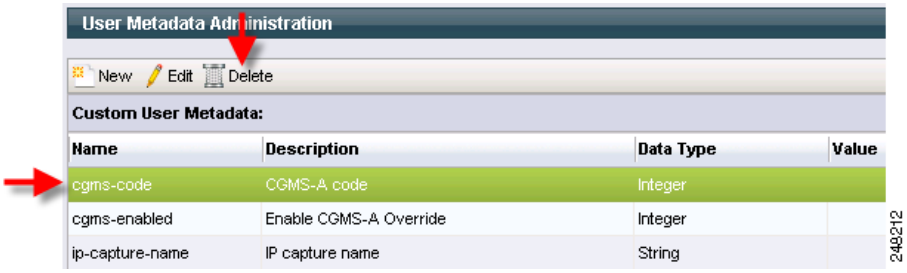
Step 3 Make any needed changes, and click **Save**. The changes will display on the User Metadata Administration page.

Deleting User Metadata

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **User Metadata** to display the page shown in Figure 14-39.

Figure 14-39 User Metadata Administration Page



Step 2 Highlight a metadata row, and click **Delete**. A confirmation pop-up displays.

Step 3 Click **OK**. The name/value pair is removed from the User Metadata Administration page.

IP Capture (Live Streaming)

Activation

To use this feature, you must purchase and install the Live Streaming feature license on the standalone Cisco MXE 3500 or the Resource Manager device.

This section includes the following topics:

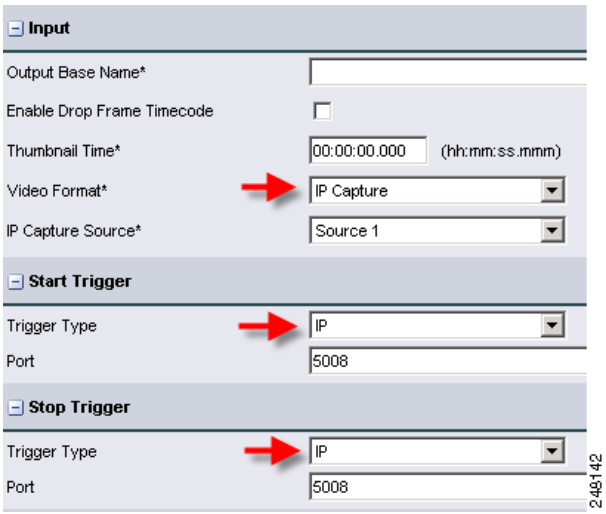
IP Capture Overview (Live Streaming)

The Cisco MXE 3500 enables ingest of live MPEG-2 and Windows media transport streams over UDP/IP with management, configuration, and status that enable general use of this feature. IP captures are limited to transport streams with MPEG-2 video and AC3/Layer2/AES3 audio essences.

Before submitting a job, you must configure the ipCapturePrefilter Worker on the Host Administration page. See also: Adding Workers to a Host, page 14-9.

In addition, on the Live Submission page, you set the Video Format to IP Capture and select the IP Capture Source (as defined in Adding an IP Capture Source (Live Streaming), page 14-40), and Start and Stop Trigger Types. See Figure 14-40.

Figure 14-40 Live Submission Page IP Capture Settings



You may send a start or stop trigger command to the running capture displayed in the Job Status Monitor (assuming start/stop IP triggers were configured with the Live Job Submission) by clicking on the Job, then **Tools > IP Trigger**.

If you are running concurrent IP captures with the same IP capture configuration along with IP triggers, you need to enter a unique ip-capture-name in the UDM field on the Live Submission page to uniquely identify the list of IP captures to send a trigger to.

On the Live Submission page, when you select the IP Capture video format, the IP Capture sources are automatically populated (from the names in the configuration page). For the selected IP Capture Source, the name will be automatically populated in the ip-capture-name UDM field. You may choose to manually override this UDM field.

Note While submitting Live jobs with IP Capture for long duration and storing output data in a file, the stop trigger should be set so that it does not overflow the disk space of the system. The stop trigger may vary depending on the encoder configuration and the actual disk space available.

Adding an IP Capture Source (Live Streaming)

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **IP Capture**.

Step 2 Click **New**. See Figure 14-41.

Figure 14-41 Creating New IP Capture Source

Step 3 In the **New IP Capture Source** pop-up, enter a unique **Name**, **IP Address**, **Port**, **Program Map PID**, and click **Create**. The new IP Capture source displays in the list. See Figure 14-42, Figure 14-43, and Figure 14-44. Table 14-14 describes the fields.

Figure 14-42 New IP Capture Source Pop-up

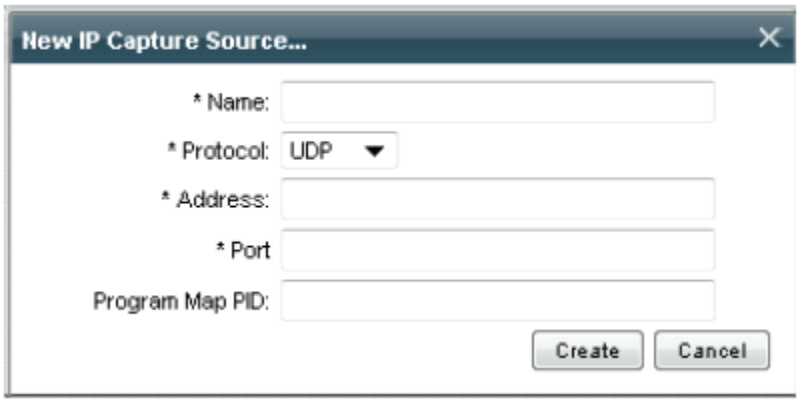


Figure 14-43 Example UDP Source Configuration

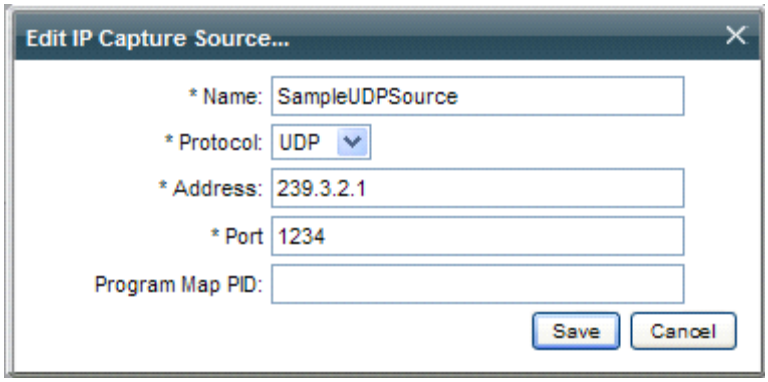


Figure 14-44 Example Windows Media Source Configuration

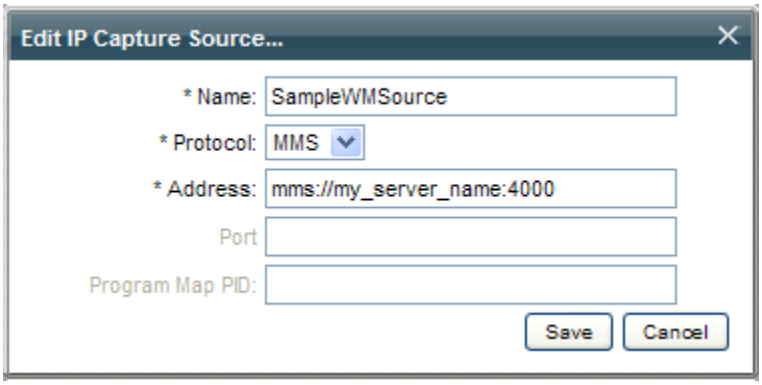


Table 14-14 IP Capture Source Fields and Descriptions

Field	Description
Name	Unique IP Capture Source name.
Protocol	Source protocol: UDP, RTP, MMS, or HTTP.
IP Address	For MPEG-2 sources: the multicast IP address of the source MPEG-2 Transport Stream. The IP addresses reserved for this purpose are from 224.0.0.0 to 239.255.255.255. For Windows Media sources: the source stream URL.
Port	The multicast port to bind to. Values range from 0 to 65535. Only applicable for UDP and RTP sources.
Program Map PID	Specifies the Program Map Table Packet ID (PMT PID) of the desired program in an MPEG-2 Multi-Program Transport Stream (MPTS). For MPEG-2 Single Program Transport Streams (SPTS) or if not specified, the first program listed in the Program Map Table is used automatically. Valid values range from 16 to 8190. Only applicable for UDP and RTP sources.

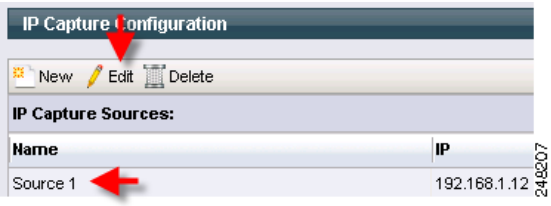
Editing an IP Capture Source (Live Streaming)

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **IP Capture**.

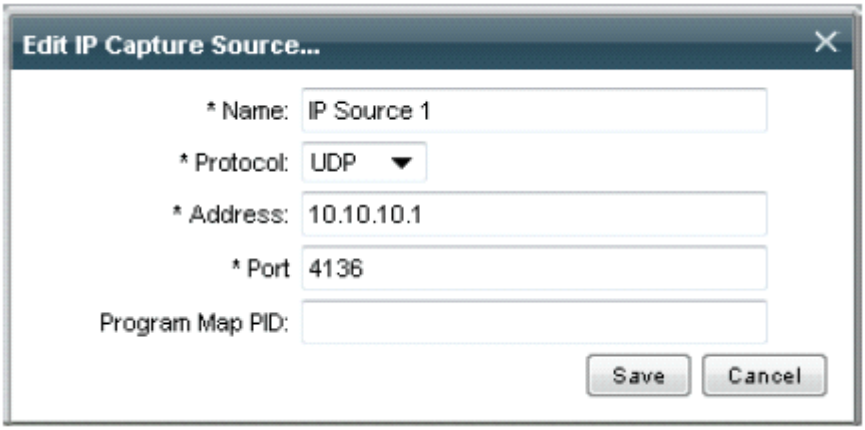
Step 2 Highlight an IP Capture source, and click **Edit**. See Figure 14-45.

Figure 14-45 Selecting IP Capture Source to Edit



Step 3 When the Edit IP Capture Source pop-up displays, make any changes to the fields, and click **Save**. See Figure 14-46. Any changes made are noted in the IP Capture Configuration pane.

Figure 14-46 Edit IP Capture Source Pop-up



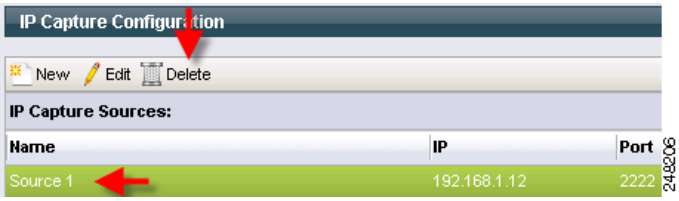
Deleting an IP Capture Source (Live Streaming)

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **IP Capture**.

Step 2 Highlight an IP Capture source, and click **Delete**. See Figure 14-47.

Figure 14-47 Selecting IP Capture Source to Delete



Step 3 When the deletion confirmation pop-up displays, click **OK**. The IP Capture source is removed from the IP Capture Configuration pane.

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.

Access the SUI administration page from the **Toolbox** by clicking **Administration > SUI Admin**.

Figure 14-48 SUI Administration Page

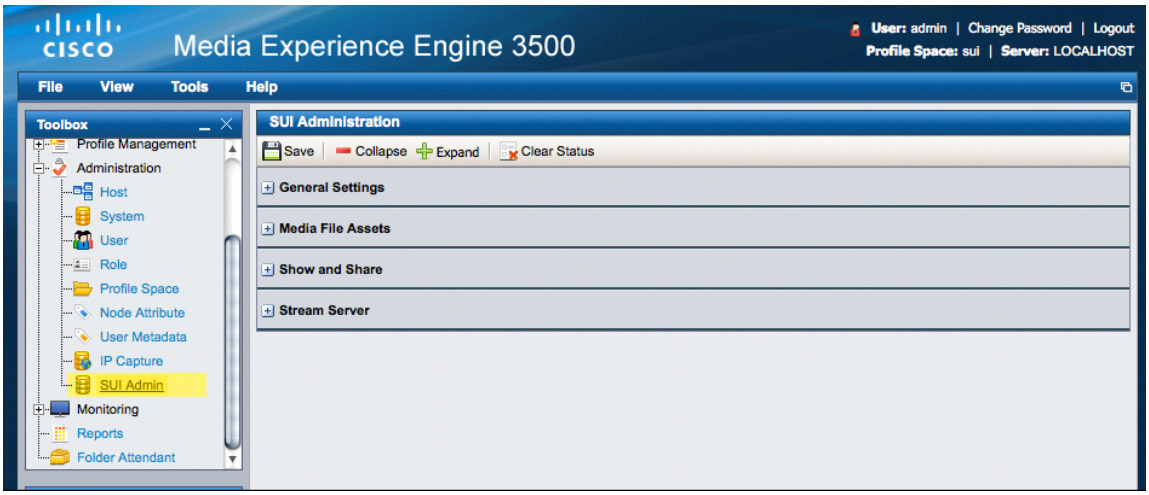


Figure 14-49 shows the General Settings section. Table 14-15 describes the settings.

Figure 14-49 General Settings Section

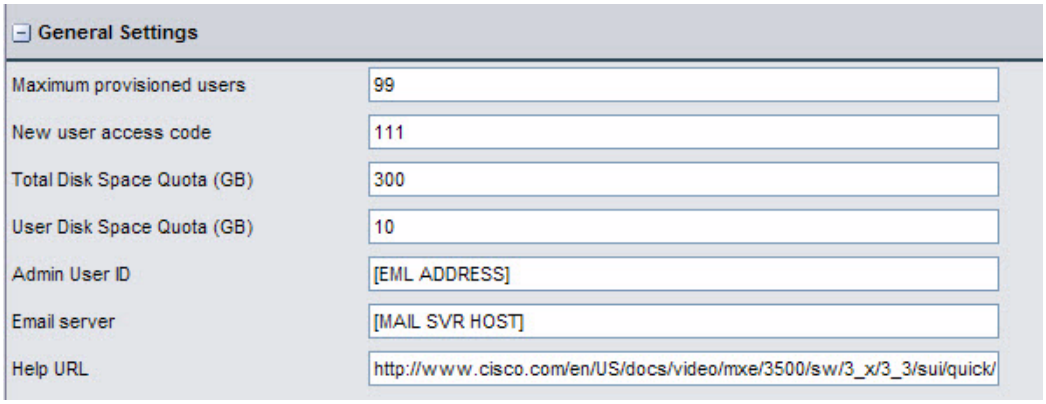


Table 14-15 General Settings and Descriptions

Field	Description
Maximum Provisioned Users	Sets the limit on users who can create accounts.
New User Access Code	Intended to prevent random users from creating accounts. The admin will provide this number to each approved user. **Note** The New user access code is used only if LDAP is not enabled. If LDAP is enabled, users log into SUI using LDAP or Active Directory credentials.
Total Disk Space Quota	Total amount of disk in GB allocated to user output storage and temporary storage. Temporary storage refers to interim files required during a conversion. These are released when a user's job completes.

Table 14-15 General Settings and Descriptions (continued)

Field	Description
User Disk Space Quota	Total amount of disk in GB reserved for each user. Does not count temporary storage while job executes.
Admin User ID	This is an e-mail address which is the 'from' address for user job completion notifications. E-mail is sent from no-reply@[MXE DOMAIN]
Email Server	Domain URL of e-mail server that you want Cisco MXE 3500 to use.

Figure 14-50 shows the Media File Assets section. Table 14-16 describes the settings.

Figure 14-50 Media File Assets Settings

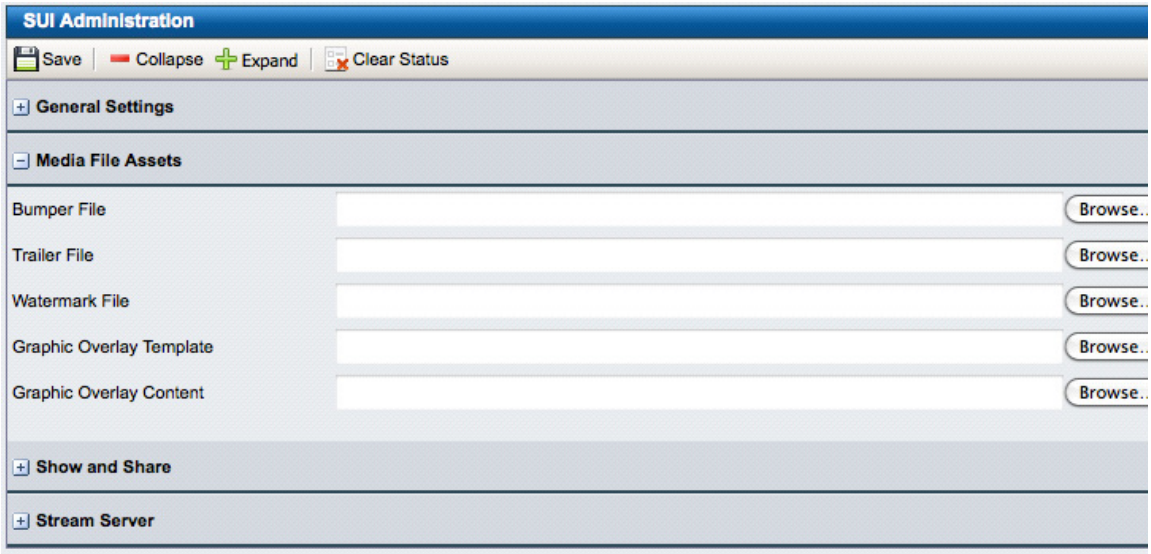


Table 14-16 Media file Assets Settings and Descriptions

Field	Description
Bumper File	Click **Browse** to select the bumper file to be attached before the user's program material in the completed conversion.
Trailer File	Click **Browse** to select the trailer file to be attached following the user's program material in the completed conversion.

Table 14-16 Media file Assets Settings and Descriptions (continued)

Field	Description
Watermark File	The file that will be superimposed on the video program as a watermark. **Note** The SUI profiles use a default, Cisco watermark file, **watermark.psd**. To **replace** and permanently delete the Cisco watermark, complete these steps: 1. Name your watermark file **watermark.psd**. 2. Upload your file. To **preserve** the Cisco watermark, choose one of these options: 1. RDC to the Windows OS. Go to the **media/assets** folder. Rename the Cisco watermark.psd file to **watermark_cisco.psd**. Name your watermark file **watermark.psd**. Then, upload your file. 2. Name your watermark file whatever you choose. Upload your file. Then, manually modify each SUI profile space preprocessor to reference this new file.
Graphic Overlay Template	A Flash SWF file that will be overlaid on the output video, showing user's text input from the Video Conversion Interface such as speaker name and speaker title.
Graphic Overlay Content	This is the XML file which is read by the overlay template SWF.

Figure 14-51 shows the Show and Share section. Table 14-17 describes the settings.

Figure 14-51 Cisco Show and Share Settings

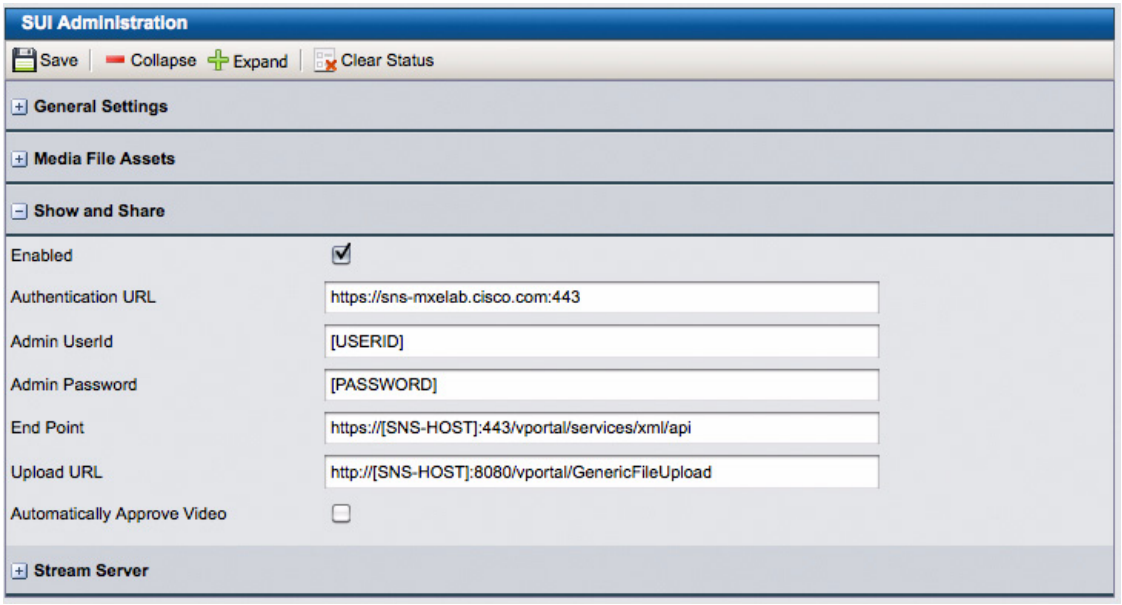


Table 14-17 Cisco Show and Share Settings and Descriptions

Field	Description
Enabled (checkbox)	Checkbox that enables upload to Cisco Show and Share, regardless of other settings present. When enabled, user will see a **Publish to Show and Share** button beside each conversion that uses an SNS file type as output.
Authentication URL	Provide the Cisco Show and Share host name and port number to allow the Cisco MXE 3500 to communicate with that server. Nominal port number is 443.
Admin Userid	The admin login name on the Cisco Snow and Share server.
Admin Password	The admin login password on the Cisco Show and Share server.
End Point	Location of the Cisco Show and Share API. Use port 443.
Upload URL	URL on the Cisco Show and Share server where user files are uploaded. Use port 8080.
Automatically Approve Video (checkbox)	Check this box to automatically approve for publication on Cisco Show and Share for all videos uploaded. If this box is not checked, uploaded videos will wait for an admin to log in and approve them.

Figure 14-52 shows the Stream Server section. Table 14-18 describes the settings.

Figure 14-52 Stream Server Settings

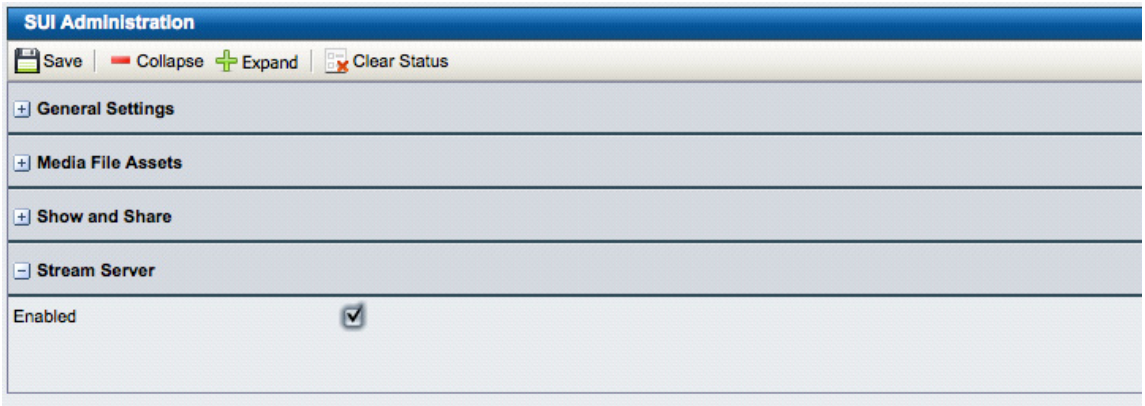


Table 14-18 Stream Server Settings and Descriptions

Field	Description
Enabled (checkbox)	Check this box to enable live streaming of live jobs processed by the Video Conversion Interface. **Note** The conversion job controlling this activity must also be configured for live streaming.

For instructions on how to use the Video Conversion Interface see *Using the Cisco MXE 3500 Release 3.3 Video Conversion Interface* on Cisco.com.

API Administration

There are two components of API administration, both affecting behavior of the Cisco MXE REST API: authentication mode and authentication password.

- Configuring Authentication Mode, page 14-48
- Changing the Authentication Password, page 14-49

Configuring Authentication Mode

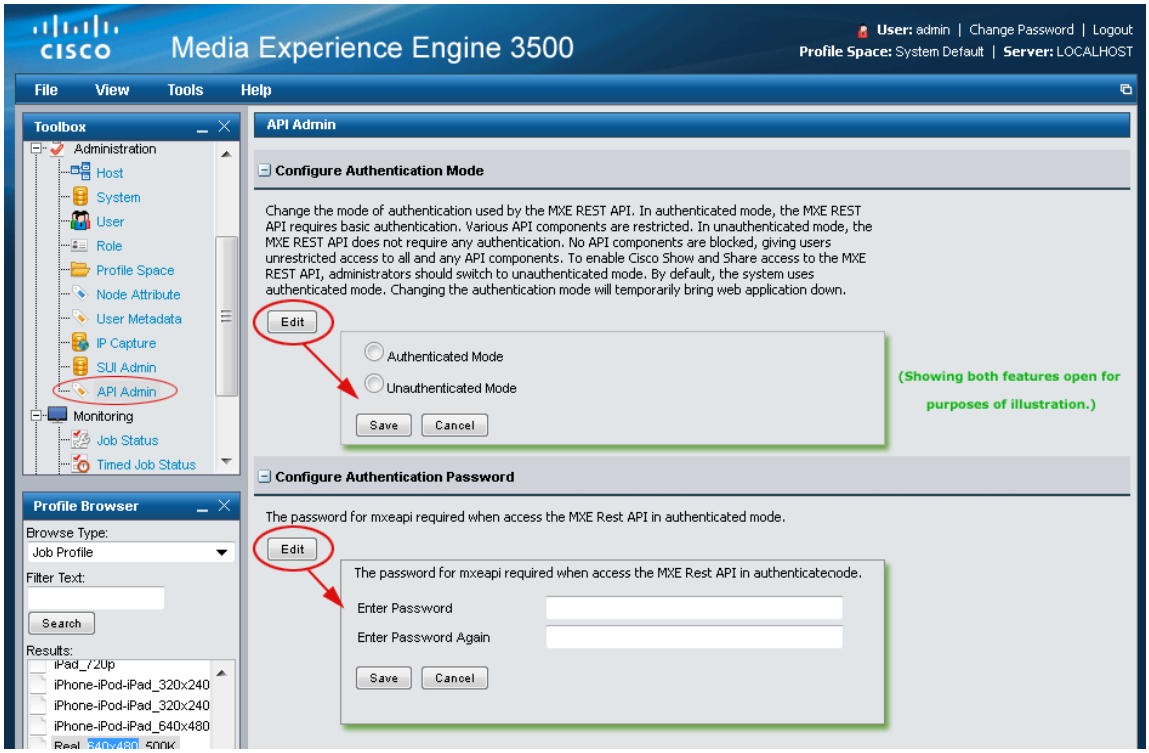
Note The authentication mode must be set to unauthenticated mode for Cisco Show and Share integration.

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **API Admin**.

Step 2 Click the **+** sign beside Configure Authentication Mode. See Figure 14-53.

Figure 14-53 API Admin Page



Step 3 Click **Edit**.

Step 4 Click **Authenticated Mode** to require basic authentication or **Unauthenticated Mode** to require no authentication.

Step 5 Click **Save**.

Changing the Authentication Password

Note For Cisco Show and Share integration, you do not need to set an authentication password.

Procedure

Step 1 From the **Toolbox**, expand **Administration**, and click **API Admin**.

Step 2 Click the **+** sign beside Configure Authentication Password. See Figure 14-53.

Step 3 Click **Edit**.

Step 4 Enter and enter again the new password in the input fields.

Step 5 Click **Save**.

LDAP Settings

Use the LDAP Settings page to configure LDAP settings. If LDAP is enabled, SUI user authentication is done with LDAP.

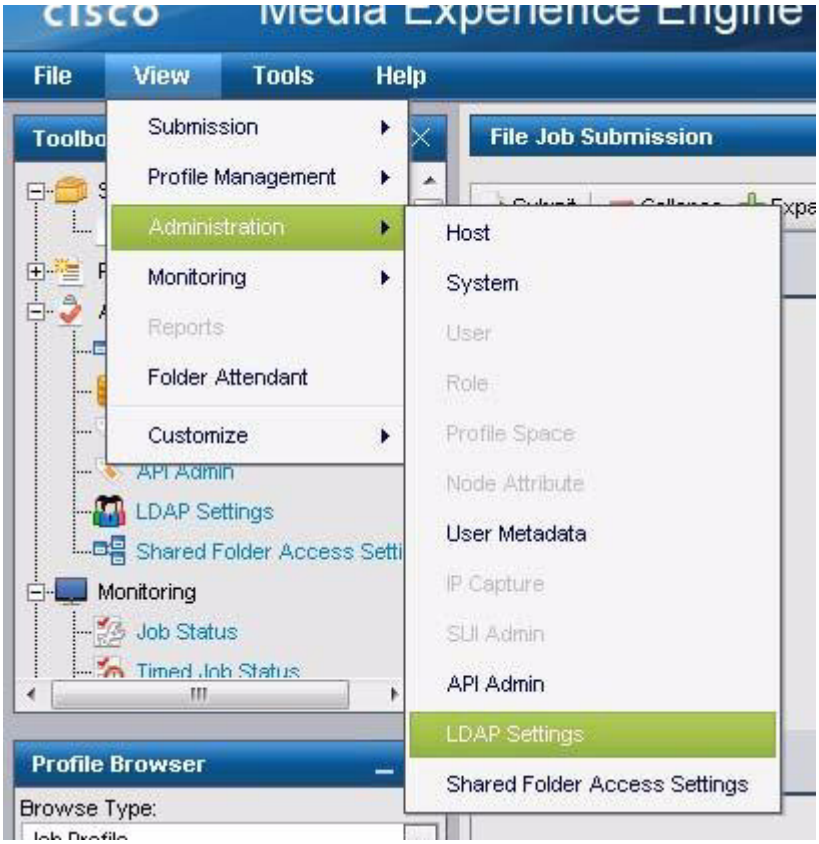
Before You Begin

- Ensure that user ID on the LDAP server that you use to authenticate the LDAP configuration settings (1) maps to an attribute that is not composite name and (2) does not require a password change at first log in. Note that the Video Conversion Interface (SUI) requires a single word—not a composite as a user ID —for authentication.
- Changes to LDAP mapping require a system reboot to restart the LDAP connection.

Procedure

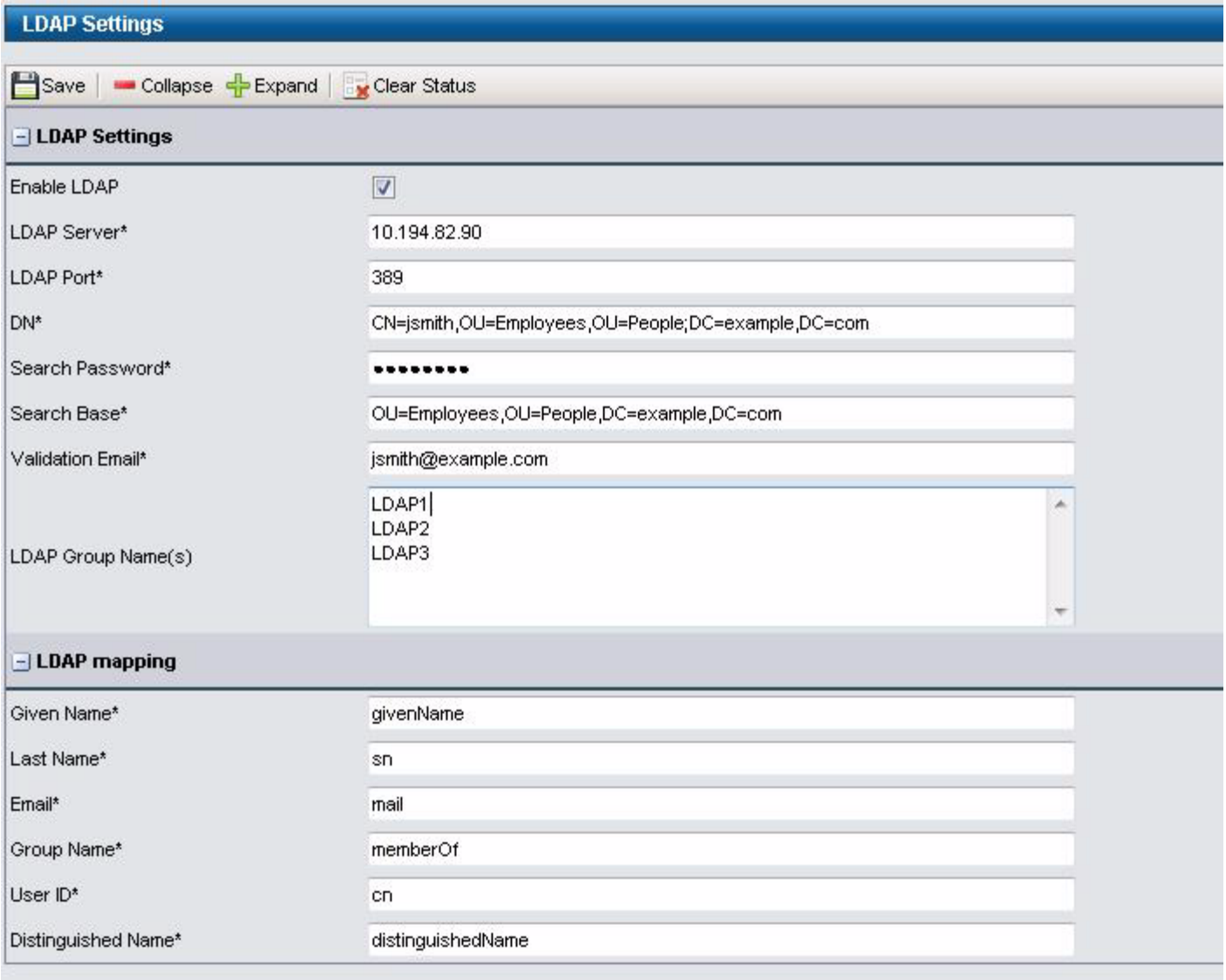
Step 1 From the **Toolbox**, expand **Administration**, and click **LDAP Settings**.

Figure 14-54 Access LDAP Settings



Step 2 Check **Enable LDAP** in the LDAP Settings page.

Figure 14-55 LDAP Settings Page



Step 3 Enter the required information in the input fields. Table 14-19 describes each field.

Note Fields with an asterisk are required.

Table 14-19 LDAP Settings and Descriptions

Field	Description
Enable LDAP (checkbox)	If **Enable LDAP** is unchecked, all LDAP settings are disabled.
LDAP Server	IP Address or the fully qualified name of the Enterprise LDAP Server. This field allows 255 alphanumeric characters.
LDAP Port	Port number to talk to the LDAP Server. This field allows numeric characters only.

Table 14-19 LDAP Settings and Descriptions

Field	Description
DN	Distinguished Name field on the LDAP Server. This field will allow 255 alphanumeric characters.
Search Password	The search password along with the email address is used to authenticate the LDAP configuration settings.
Search Base	Search base field on the LDAP Server. This field allows 255 alphanumeric characters.
Validation Email	Valid email address. The email address is used to log in to the LDAP Server and validate the LDAP configuration. This field allows 255 alphanumeric characters.
(Optional) LDAP Group Names	If no group is defined, all users from the domain, up to the maximum defined in the SUI Admin, are allowed to create an account. Maximum number of groups allowed is 10. List each group name on a separate line. Provide the complete group name, for example: CN=LDAP1_all,OU=Employees,OU=People,DC=example,DC=com **Note** The system does not validate the LDAP Group Names.
LDAP Mapping	
Given Name	LDAP given name mapping. This field allows 255 alphanumeric characters.
Last Name	LDAP last name mapping. This field allows 255 alphanumeric character
Email	LDAP email mapping.
Group Name	LDAP group name mapping. This field allows 255 alphanumeric characters. **Note** The system validates group name mapping only if the LDAP group names are listed in the LDAP Group Names field.
User ID	LDAP user ID mapping. This field allows 255 alphanumeric characters. **Tip** Instead of using the default “cn” attribute, you can use the “sAMAccountName” attribute. The “cn” is a composite of last name and first name, such as John Doe, whereas “SAMAaccountName” is a single word (johndoe), which the SUI requires for authentication.
Distinguished Name	LDAP DN mapping.

Step 4 Click **Save**.

Shared Folder Access Settings

Use this feature to configure access to shared folders. This sections contains the following topics:

- Shared Folder Access Settings Page, page 14-53
- Configuring Access to Shared Folders, page 14-54

Shared Folder Access Settings Page

From the **Toolbox**, expand **Administration**, and click **Shared Folder Access Settings**. Figure 14-56 shows the Shared Folder Access Settings page.

Figure 14-56 Shared Folder Access Settings Page

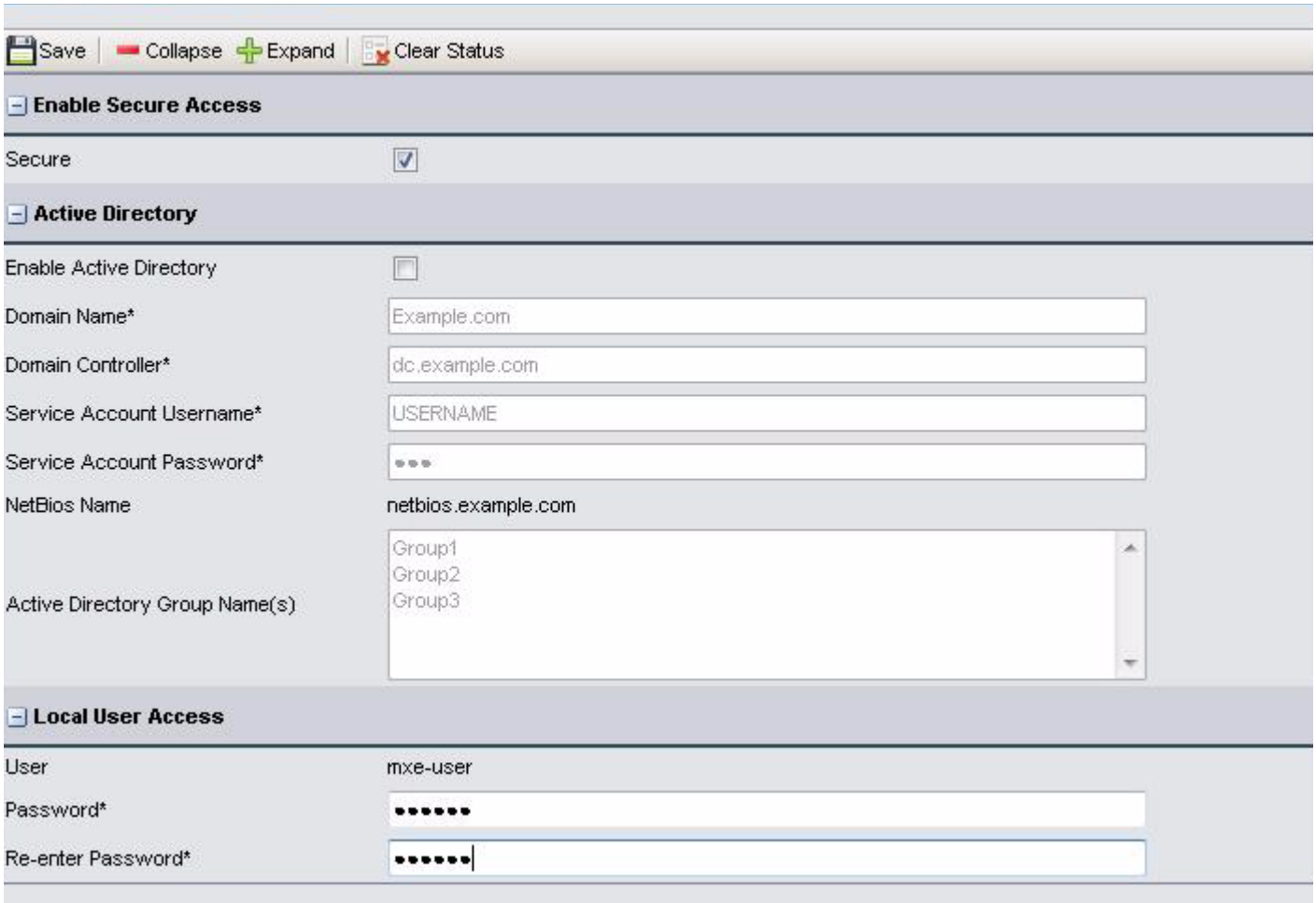


Table 14-20 describes the Active Directory fields.

Table 14-20 AD Settings and Descriptions

Field	Description
Enable Active Directory (checkbox)	Check this field to Enable AD integration.
Domain Name	The AD domain name.
Domain Controller	The AD domain controller.
Service Account User Name	Valid AD user ID. This ties the Cisco MXE 3500 with the AD domain.

Table 14-20 AD Settings and Descriptions

Field	Description
Service Account Password	Valid AD password for the Service Account User Name. This ties the Cisco MXE 3500 with the AD domain.
NetBios Name	The Cisco MXE 3500 hostname. This name must match the Cisco MXE 3500 hostname configured in AD.
(Optional) Active Directory Group Name(s)	List one or more group names allowed access to the shared folders. List each group name on a separate line. Each group name must be a valid group in the AD. Maximum number of groups allowed is 10. If no group is specified, all users in the AD domain will have access to the shared folders.

Configuring Access to Shared Folders

Configure access to the shared folders in one of the following modes:

- Open Access Mode, page 14-54
- Active Directory Mode, page 14-54
- Local User Access Mode, page 14-56

Open Access Mode

The open access mode is the default mode for accessing the MXE 3500 shared folders. In this mode, users do not need a username and password to access the shared folders.

To enable this mode, uncheck the **Secure** option in the Enable Secure Access section of the Shared Folder Access Settings page.

Active Directory Mode

- About Active Directory Mode, page 14-54
- Before You Begin, page 14-55
- Enable Active Directory Mode, page 14-55
- Disable Active Directory Mode, page 14-56

About Active Directory Mode

The Active Directory (AD) mode allows users access to the Cisco MXE 3500 shared folders with their Enterprise domain login credentials.

Integrating with AD eliminates the need to maintain users and their account details on the Cisco MXE 3500 appliance. Users can access the following using their Enterprise login credentials:

- The Cisco MXE 3500 Video Conversion Interface. The username and password are verified against the LDAP server in the Enterprise.
- The Cisco MXE 3500 shared folders (watch, media, output, temp, and folders shared for a standalone or RM appliance).

Note The AD settings are saved on the Windows OS under c:\mxe\config with filename activedirectory.properties.

Note If AD is enabled, the administrator manages the **mxe-service** account and password.

Before You Begin

- Ensure that the NTP server is configured. If the NTP server is not configured, see Modifying Network Settings and Admin Password, page 4-2.
- Identify or create an account in the AD that is authorized to join the Cisco MXE 3500 to the AD domain.

  The applications on the Cisco MXE 3500 run as a service. These services are associated with the preconfigured **mxe-service** user . When AD is implemented, the user associated with the Cisco MXE 3500 services must be changed to a user configured in the AD system.

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**.

Step 3 Enter the required information in the input fields.

Tip Fields with an asterix are required.

Step 4 Click **Save**.

Step 5 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 6 At the Command Prompt, enter **AddServiceUser** *username password.* The *username* and *password* are the Service Account Username and Password entered in Step 3.

The AddServiceUser.bat script creates the new user on the Windows platform. It then associates all Cisco MXE 3500 services to the new user.

Step 7 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.

Disable Active Directory Mode

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

Step 1 Uncheck **Enable Active Directory**.

Step 2 Click **Save**.

Step 3 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 4 At the Command Prompt, enter **RestoreServiceUser mxe-service** *password.* The *password* is the password for the **mxe-service** user.

Step 5 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

The local user access mode allows users access to the MXE 3500 shared folders with a single username and password combination that is set to **mxe-user**. Users are provided the option to update the password for the shared folder account.

Enterprises that do not have an AD or choose not to tie the system with the AD use this mode to secure access to the shared folders.

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**.

Additional Administrative Tools

In addition to the administrative tools available on the main the Web User Interface (UI), the Cisco MXE 3500 offers additional features:

- Cisco MXE 3500 Tools, page 14-57: Allows you to preview Preprocessor Profile clips or create/edit QuickTime Encoder Profiles
- Profile Converter, page 14-58: Normalizes any pre-existing profiles you may have into formats that are acceptable to the current Profile Editor, thereby preventing profile-related job failures.
- Database Configuration, page 14-66: A simple management utility that allows you to set up, configure, migrate, and update your Cisco MXE 3500 database.

- Log Viewer, page 14-67: Allows you to view events taking place across a Cisco MXE 3500 installation.

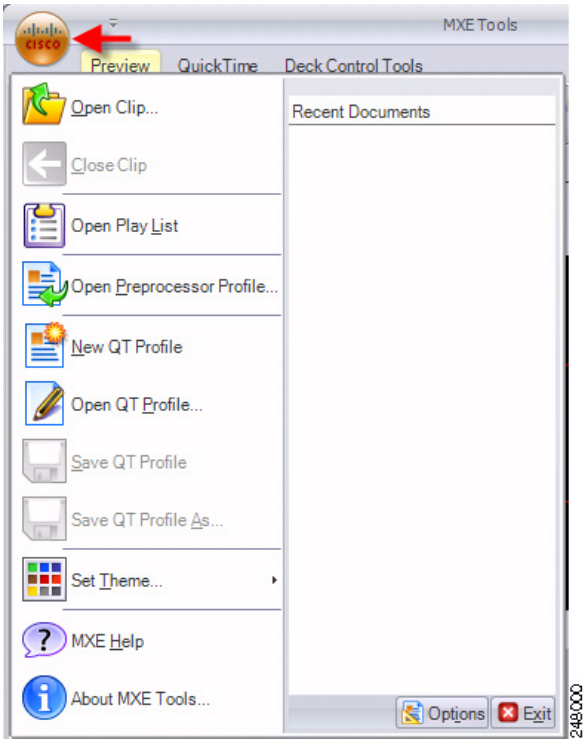
Cisco MXE 3500 Tools

To access Cisco MXE 3500 Tools, click on the Cisco desktop icon or click **Start** > **All Programs** > **Cisco** > **Media Experience Engine** > **Media Experience Engine Tools**.

Note The Cisco MXE 3500 Tools feature does not work interactively with the Cisco MXE 3500 UI.

Click the Cisco icon in the upper left corner to view the Cisco MXE 3500 Tools menu. See Figure 14-57.

Figure 14-57 Accessing Cisco MXE 3500 Tools Options



See also:

- Previewing Preprocessor Clips, page 6-40
- Creating a QuickTime Encoder Profile, page 8-53
- Editing a QuickTime Encoder Profile, page 8-54

Setting Independent Profile Space

The Cisco MXE 3500 Tools application has the ability to set a profile space independently of the Cisco MXE 3500 UI profile space.

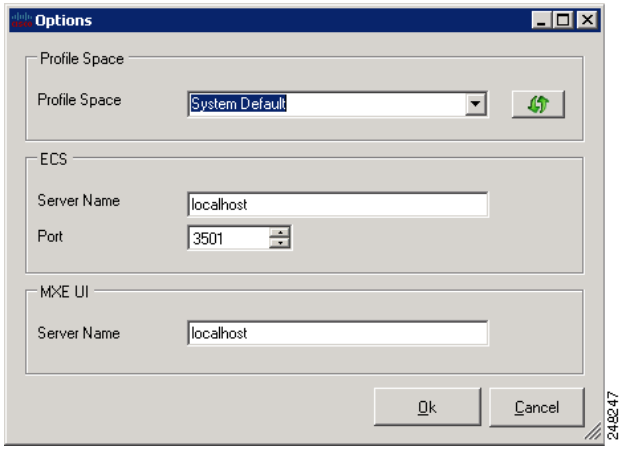
Procedure

Step 1 Launch Cisco MXE 3500 **Tools**.

Step 2 Click the Cisco icon in the upper left corner.

Step 3 Click **Options** in the lower right corner. See Figure 14-58.

Figure 14-58 Tools Options



Step 4 From the drop-down, select the **Profile Space** you want to use.

Note Specify the Server Name and Port of the system when Cisco MXE 3500 Tools is installed on an LCS node (controlling the deck) and the ECS, and Cisco MXE 3500 UI are installed on separate machines. Otherwise the ECS and UI Server Names are typically the same.

Profile Converter

The purpose of the Cisco MXE 3500 Profile Converter is to update, through a Wizard, pre-existing profiles so that they are editable by someone using the Cisco MXE 3500 UI. The Profile Converter applies dependency rules and defaults that normalize the profiles and ensure that they will be acceptable to the current Profile Editor in the MXE 3500 UI.

In addition to making the profiles compatible with the Cisco MXE 3500, the Profile Converter sets proper defaults and corrects for settings that do not fall into the valid range of values. For example, a setting that is out of range may be corrected, or a tag may list a feature that does not exist in the profile definition.

Converted profiles should be evaluated and tested to verify that any changes made during the conversion produce the expected transcoding results in the Cisco MXE 3500. The Profile Converter produces an upgrade log that is written to the root of the selected profile directory before the wizard exits. The upgrade log is an HTML document that can be viewed with a browser. It displays changes and modifications made to each profile, as well as errors that may have occurred during processing.

Note Profile customizations that are made by manual editing of XML will not be preserved by the conversion process, and their omission will not be reported in the log file. If profiles are not converted, the UI Profile Browser may not be able to load them. However, while not editable, these profiles are compatible for use with the Cisco MXE 3500.

When the Profile Converter runs, it makes a back-up of any profile that it changes. The back-ups are located in the same directory as the profile that was updated with a .bak file extension.

Note The user running the Profile Converter must have write permission to the profile directory being converted.

See also: Profile Converter Log Entries, page 14-61.

Running the Profile Converter

The Profile Converter scans one profile directory at a time and scans for files to upgrade to Cisco MXE 3500 profile standards. The converter is a wizard that runs in several stages:

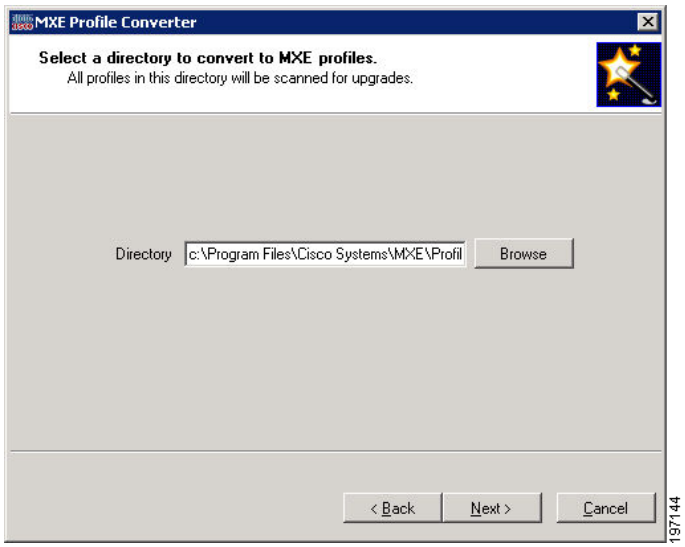
Procedure

Step 1 Click **Start > All Programs > Cisco > Media Experience Engine > Media Experience Engine Profile Converter**. The Welcome screen displays. See Figure 14-59.

Figure 14-59 Profile Converter Welcome Screen

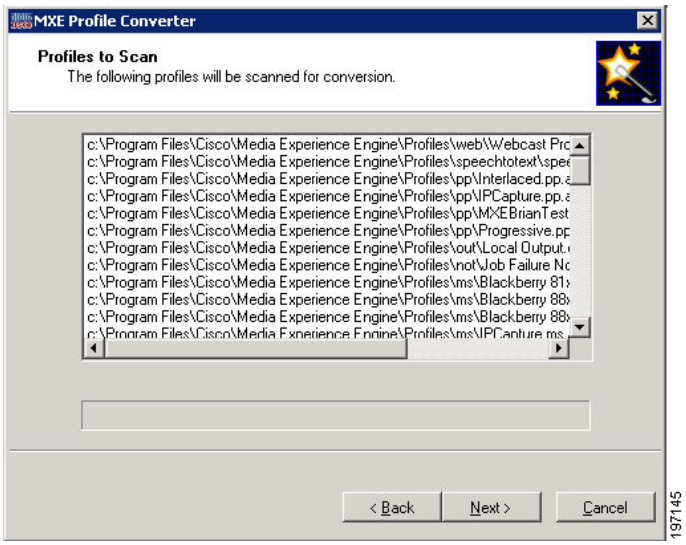
Step 2 Click **Next**. At the next screen, Browse to the location of the profiles you want to convert. See Figure 14-60.

Figure 14-60 Selecting the Profile Directory



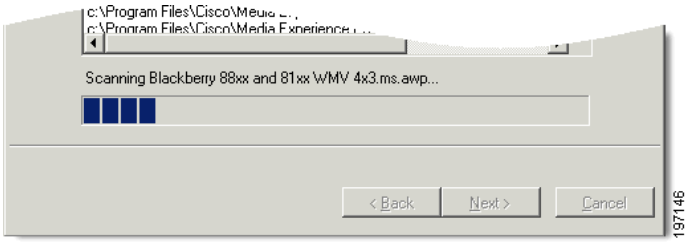
Step 3 Click **Next**. A list of profiles that will be scanned displays. Review the list, and click **Next**. See Figure 14-61.

Figure 14-61 Profiles to Scan List



Step 4 The bar shows the progress of the scan. See Figure 14-62.

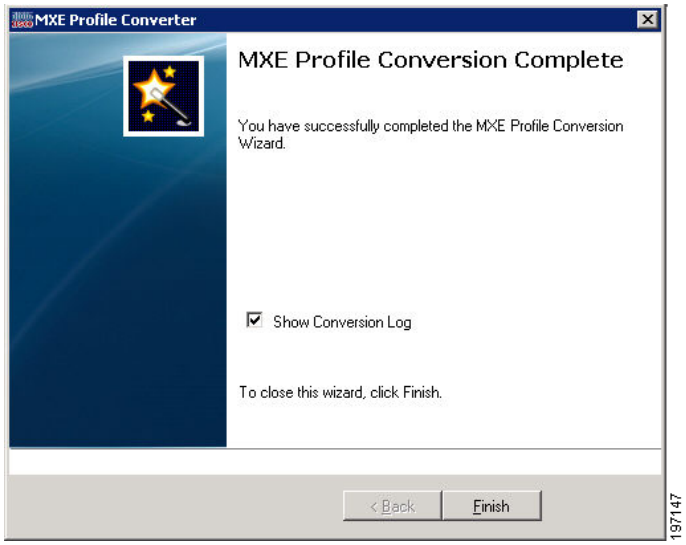
Figure 14-62 Scan Progress Bar



Step 5 When the scan is complete, the Profile Converter displays a list of **Profiles that Require Conversion**. Review the list, and click **Next**.

Step 6 When the conversion is complete, the **Profile Conversion Complete** screen displays. If you want to view the Conversion Log, check the box, and click Finish. If not, uncheck the box, and click **Finish**. See Figure 14-63.

Figure 14-63 Profile Conversion Complete



Profile Converter Log Entries

When you run the Profile Converter, a conversion log is produced. The log contains two main types of log messages:

- The largest number of log messages are tag additions. New tags never cause a problem, and the log message is informational only.
- The second main class of messages is value change. In many cases the profile value was incorrect, and in some cases, the correct value could not be determined. In these cases, the default value is set and the change logged. These messages should be examined closely since you may need to open the profile and reset the specific parameter that was changed by the Profile Converter.

Table 14-21 describes the log entries.

Table 14-21 Profile Converter Log Entries Descriptions

Log Entry	Description	Tag(s)
FL8 and Flash	Incorrectly fixes UI bug that mismatched output-format and output-extension values. The Profile Converter changes Flash-8-FLV to Flash-8-SWF to match incorrect swf extension. It should change swf to flv.	parameters.output-format
FL8	These three tag values contained the list values not the selected value in two profiles. The Profile Converter chooses the default. It is not possible to determine what the desired values were.	export.output.extension parameters.output-format parameters.video.codec
FL8	parameters.video.bit-rate-control.override-quantizer is changed to correct tag name	parameters.video.bit-rate-control.quality parameters.video.bit-rate-control.quality
FL8	Correctly changes bitrate control values that are higher than allowed to the maximum value.	parameters.video.bitrate-control.quality
FL8	Correctly changes export max video bitrate value to match the parameters value.	export.encoder.max-video-bitrate
FL8	Correctly changes export max height value to match the parameters value.	export.encoder.max-height
FL8	Correctly adds numerous new tags, for example	parameters.grid parameters.video.keyframe-control parameters.video.bitrate-control.peak-bit-rate parameters.video.fixed-quality.enabled parameters.video.temporal-resampling.enabled
FL8	Incorrectly handles export max audio bitrate values set to 0. The export value is changed to the default value [32] and then the parameters audio bitrate value is set to the default value that the export parameter was set to [32]. If a conversion log has this issues, the profile must be hand edited to set the max audio bitrate export value to the correct value from the parameters audio bitrate.	parameters.audio.bit-rate export.encoder.max-audio-bitrate
H.264	Fixes bad worker parameters. Constant quality encode mode is no longer dependant on encode mode VBR and avg. bit rate 0. When converted, it uses only encode mode = VBR-CQT.	parameters.video.bit-rate-control.mode
H.264	Correctly fixes export audio bitrate value.	export.encoder.max-audio-bitrate

Table 14-21 Profile Converter Log Entries Descriptions (continued)

Log Entry	Description	Tag(s)
H.264	Correctly adds numerous new tags, for example:	parameters.video.write-sequence-parameter-set parameters.subtitles + all subtags to this parameters.video.vbv-buffer.initial-fullness parameters.video.aspect-ratio.enabled parameters.video.advanced-settings.cr-offset parameters.video.scene-change-detection.mode
MPEG	Incorrectly sets parameters channel mono value to stereo to match export.encoder value. The export block value is incorrect due to a UI bug that always sets the export block to stereo.	parameters.audio.codec.channels export.encoder. audio-channels
MPEG	Correctly restores Layer 2 so that no conversion is necessary on the type. Because the audio bitrates are updated, it is possible that the audio bitrate can be correctly changed.	parameters.audio.bit-rate export.encoder.max-audio-bitrate
MPEG	Correctly adds new tags, for example:	parameters.video.afd.enabled parameters.video.afd.value parameters.subtitles + all subtags to this parameters.video.vbv-buffer-type parameters.video.vbv-buffer-size
MPEG	Incorrectly sets the multiplexer stream value for profiles created in previous interfaces. The previous interface used a numeric stream-display value while the new UI uses a string value. The stream-display parameter was used by the UI only because of the limitations of the previous UIs. The new UI does not have this limitation, and the stream-display parameter is obsolete. The profile can be hand edited to remove the value, or set to the correct string value from the previous UI.	parameters.multiplexer.stream parameters.multiplexer.stream-display

Table 14-21 Profile Converter Log Entries Descriptions (continued)

Log Entry	Description	Tag(s)
MPEG	Unintended FTP value conversion Action: Modify Tag: parameters.video.fps Old Value: 23.97 New Value: 29.97 Action: Modify Tag: export.encoder.max-fps Old Value: 23.97 New Value: 29.97 Problem: 23.97 is not a valid value. If the MPEG profile was created using an ASP.UI, the profile may save this 23.97 value. 29.97 is the default. Solution: Edit profile in the new UI to 23.976	parameters.video.fps export.encoder.max-fps
MPEG	Unintended audio channels conversion Action: Modify Tag: parameters.audio.codec.channels Old Value: stereo New Value: mono Problem: There are two competing values in the profile: 1) export.encoder.audio-channels = stereo 2) parameters.audio.code.channels = mono Trying to load a profile in the UI results in a profile error: "Drop-down control 'mpegAChannels' cannot be mapped with the given values from its tags." Solution: Set profile export block manually to the value of mono.	parameters.audio.codec.channels
MPEG	Incorrectly changes sample rate values if sample rate is not equal to 44.1 hz in parameters.audio(1-8).codec.sample-rate blocks. The profile contains a sample rate value in each audio group, but currently all sample rates must be the same. Thus, any values other that 44.1 hz will be changed by the setting of the audio groups 2-8 sample rate default values.	parameters.audio.codec.sample-rate
MS	Correctly adds numerous new tags, for example:	parameters.video.aspect-ratio.enabled parameters.video.aspect-ratio.type parameters.video.aspect-ratio.x-ratio parameters.video.aspect-ratio.y-ratio

Table 14-21 Profile Converter Log Entries Descriptions (continued)

Log Entry	Description	Tag(s)
MS	Incorrectly handles previous UI bug where targets 2-5 have incorrect precision (2 instead of 3) for max-fps. The Profile Converter uses the truncated target value instead of the correct export value.	export.encoder.max-fps parameters.target.video.max-fps
PP	Correctly fixes bug where list of keys was saved out as default value and not 1 (first key).	parameters.video.philips-forensic-watermark.key-index
PP	Correctly adds numerous new tags, for example:	Parameters.video.motion-compensation Parameters.video.vertical-shift.num-lines Parameter.burn-in.subtitiles.enabled
PP	Correctly fixes audio low pass values that exceed the maximum to the maximum allowed value.	parameters.audio.low-pass
PP	Correctly fixes the field parameters.video.unsharp-mask-radius, correcting cases where the unsharp mask radius was greater than the maximum allowed value.	parameters.video.unsharp-mask-radius
PP	Correctly fixes an issue with the field parameters.burn-in.timecode.font-height-pct, where the profile had a value that was below the minimum allowed value for this field.	parameters.burn-in.timecode.font-height-pct
PP	Correctly fixes cases where parameters.video.watermark[1].height is greater than the maximum allowed value for the field.	parameters.video.watermark[1].height
PP	Correctly fixes cases where export.encoder.fast-start equaled No instead of 1.	export.encoder.fast-start
PP	Correctly fixes cases where parameters.video.color-range is Off instead of Pass. (Off is the displayed value and not the correct saved value for this field).	parameters.video.color-range
QT	UI fps values can have several bugs. 1) the 404 patch bug with fps truncated to two decimal places. 2) the export block value is incorrectly translated by string to decimal function and contains extra decimal places. 3) when using QuickTime API values, the parameters fps value is not updated, creating conflicting values. The Profile Converter uses the correct export value.	parameters.media.target-fps export.encoder.max-fps
QT	UI channel values can differ when using QuickTime API values. The previous UI did not update the parameters value with the API value, only the export block. If the two are different, the Profile Converter uses the correct export block value.	parameters.media.audio.channels export.encoder. audio-channels

Table 14-21 Profile Converter Log Entries Descriptions (continued)

Log Entry	Description	Tag(s)
REAL	Correctly adds numerous new tags, for example:	export.encoder.archive export.encoder.immediate parameters.audio.tracks.track-1 parameters.complexity parameters.startup-latency parameters.quality parameters.target[x].video.maxbit-rate
REAL	Audio bitrate and sample rate values are modified to the default value. When this occurs, the value in the profile is not valid for the latest music/voice value lists. Thus, the default values are substituted. This case is almost always in disabled targets 2-5, meaning it has no effect on the encoded output. In other rare cases, the default values are incorrect and should be manually modified to the closest valid value.	
WAV	Correctly fixes previous UI bug that used incorrect values for sample rate and sample size to compute max-audio-bitrate.	export/encoder/max-audio-bitrate
WEBCAST	Correctly adds missing tags with the correct default values. This includes profiles with only five server tags; The Profile Converter adds five more and child tags.	parameters.server[x].server-cdn parameters.server[6-10].enabled parameters.server[6].user-password

Database Configuration

The Database Configuration Tool is normally used during the installation process to set up, configure, and migrate databases. However, it may also be used by administrators needing to update or maintain their database.

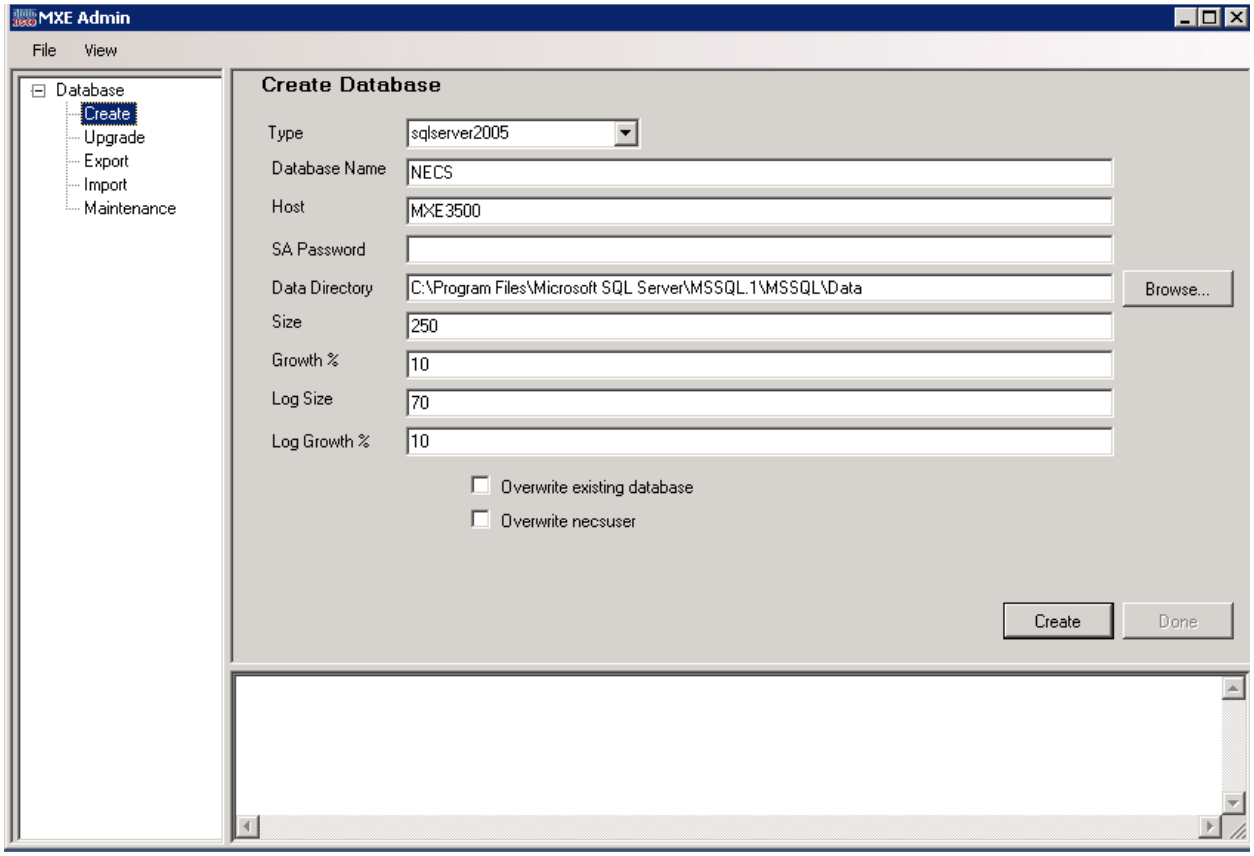
This tool offers a simple user interface that allows you to:

- Create a new, properly configured Cisco MXE 3500 production database.
- Upgrade replaces Cisco MXE 3500 production database with a newer version
- Export the system configuration information to an external file. This preserves system setup and customization data.
- Import previously stored system configuration information for reconfiguring new or updated systems.
- Remove old job information. You define purging parameters.

To access the Cisco MXE 3500 Database Configuration tool

- Click **Start > All Programs > Cisco > Media Experience Engine > Media Experience Engine Configuration**. See Figure 14-64.

Figure 14-64 Database Configuration Tool



Log Viewer

The Log Viewer is not supported in Release 3.2.